U.S. Intelligence Law

Administrative Law Supplement
(2nd Edition 2013)

By

David Alan Jordan
Editor-in-Chief
IntelligenceLaw.com

IntelligenceLaw.com Supplement Series

United States of America, 2013
To the Center for Democracy & Technology and OpenCRS.com
[www.cdt.org & http://opencrs.com]
Preface

This supplement contains legislative and non-legislative administrative rules relevant to U.S. Intelligence Law.

DAVID ALAN JORDAN

January, 2013
Summary of Contents

Preface ................................................................. 4
Summary of Contents ........................................... 5
Chapter-Level Table of Contents ......................... 7
Full Table of Contents ........................................ 13
PRESIDENTIAL RULES ........................................ 57
  Executive Order 10865. Safeguarding Classified Information Within Industry .................................... 58
  Executive Order 12139. Exercise of Certain Authority Respecting Electronic Surveillance ...................... 63
  Executive Order 12333. United States Intelligence Activities ......................................................... 65
  Executive Order 12829. National Industrial Security Program ......................................................... 95
  Executive Order 12937. Declassification of Selected Records Within National Archives of United States ................................................. 103
  Executive Order 12949. Foreign Intelligence Physical Searches ......................................................... 105
  Executive Order 12951. Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems ................................................. 107
  Executive Order 12968. Access to Classified Information .............................................................. 109
  Executive Order 13353. Establishing the President's Board on Safeguarding Americans' Civil Liberties ......................................................... 125
  Executive Order 13434. National Security Professional Development ......................................... 129
  Executive Order 13462. President's Intelligence Advisory Board and Intelligence Oversight Board ......................................................... 133
  Effective Dates of Provisions in Title I of the Intelligence Reform and Terrorism Prevention Act of 2004 ......................................................... 140
  Executive Order 13467. Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information ......................................... 143
  Executive Order 13491. Ensuring Lawful Interrogations .............................................................. 152
  Executive Order 13526. Classified National Security Information ..................................................... 157
Executive Order 13549. Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities 196
Executive Order 13556: Controlled Unclassified Information (Nov. 4, 2010) 204
Executive Order 13587. Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information 208
Implementation of the Executive Order, “Classified National Security Information” 215
Original Classification Authority 218

**LEGISLATIVE AGENCY RULES** 221
CFR TITLE 28—JUDICIAL ADMINISTRATION 222
CFR TITLE 32—NATIONAL DEFENSE 871

**NON-LEGISLATIVE AND OTHER AGENCY RULES** 1244
Department of Defense Regulation 5240.1-R: Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons 1245
Department of Defense Directive 5240.01 1302
The Attorney General’s Guidelines for Domestic FBI Operations 1308

**JUDICIAL BRANCH RULES** 1347
Foreign Intelligence Surveillance Court Rules 1348
Alien Terrorist Removal Court Rules 1363
# Chapter-Level Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Summary of Contents</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Chapter-Level Table of Contents</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Full Table of Contents</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>PRESIDENTIAL RULES</td>
<td></td>
<td>57</td>
</tr>
<tr>
<td>Executive Order 10865. Safeguarding Classified Information Within Industry</td>
<td></td>
<td>58</td>
</tr>
<tr>
<td>Executive Order 12139. Exercise of Certain Authority Respecting Electronic Surveillance</td>
<td></td>
<td>63</td>
</tr>
<tr>
<td>Executive Order 12333. United States Intelligence Activities</td>
<td></td>
<td>65</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PART 1—GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS</td>
<td></td>
<td>66</td>
</tr>
<tr>
<td>PART 2—CONDUCT OF INTELLIGENCE ACTIVITIES</td>
<td></td>
<td>85</td>
</tr>
<tr>
<td>PART 3—GENERAL PROVISIONS</td>
<td></td>
<td>90</td>
</tr>
<tr>
<td>Executive Order 12829. National Industrial Security Program</td>
<td></td>
<td>95</td>
</tr>
<tr>
<td>PART 1. ESTABLISHMENT AND POLICY</td>
<td></td>
<td>95</td>
</tr>
<tr>
<td>PART 2. OPERATIONS</td>
<td></td>
<td>98</td>
</tr>
<tr>
<td>Executive Order 12937. Declassification of Selected Records Within National Archives of United States</td>
<td></td>
<td>103</td>
</tr>
<tr>
<td>Executive Order 12949. Foreign Intelligence Physical Searches</td>
<td></td>
<td>105</td>
</tr>
<tr>
<td>Executive Order 12951. Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems</td>
<td></td>
<td>107</td>
</tr>
<tr>
<td>Section 1. Public Release of Historical Intelligence Imagery.</td>
<td></td>
<td>107</td>
</tr>
<tr>
<td>Sec. 2. Review for Future Public Release of Intelligence Imagery.</td>
<td></td>
<td>107</td>
</tr>
<tr>
<td>Sec. 3. General Provisions.</td>
<td></td>
<td>108</td>
</tr>
<tr>
<td>Sec. 4. Definition.</td>
<td></td>
<td>108</td>
</tr>
<tr>
<td>Executive Order 12968. Access to Classified Information</td>
<td></td>
<td>109</td>
</tr>
<tr>
<td>PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS</td>
<td></td>
<td>109</td>
</tr>
<tr>
<td>PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE</td>
<td></td>
<td>114</td>
</tr>
<tr>
<td>PART 3—ACCESS ELIGIBILITY STANDARDS</td>
<td></td>
<td>117</td>
</tr>
</tbody>
</table>
Executive Order 13526. Classified National Security Information ____ 157
PART 1—Original Classification ........................................ 157
PART 2—Derivative Classification ......................................... 165
PART 3—Declassification and Downgrading .......................... 167
PART 4—Safeguarding ..................................................... 178
PART 5—Implementation and Review ................................ 182
PART 6—General Provisions ............................................. 188

Executive Order 13549. Classified National Security Information Program
for State, Local, Tribal, and Private Sector Entities ................. 196
Section 1. Establishment and Policy. .................................. 196
Sec. 2. Policy Direction. .................................................. 198
Sec. 3. SLTPS Policy Advisory Committee. ......................... 198
Sec. 4. Operations and Oversight. ..................................... 199
Sec. 5. Definitions. ....................................................... 200
Sec. 6. General Provisions. ............................................. 202
Sec. 7. Effective Date. ................................................... 203

Executive Order 13556: Controlled Unclassified Information (Nov. 4, 2010) 204
Section 1. Purpose. ....................................................... 204
Section 2. Controlled Unclassified Information (CUI). ............ 204
Section 3. Review of Current Designations. ......................... 204
Section 4. Development of CUI Categories and Policies. ........ 205
Section 5. Implementation. ............................................. 206
Section 6. General Provisions. ......................................... 206

Executive Order 13587. Structural Reforms To Improve the Security of
Classified Networks and the Responsible Sharing and Safeguarding of
Classified Information .................................................... 208
Section 1. Policy. ......................................................... 208
Sec. 2. General Responsibilities of Agencies. ....................... 208
Sec. 3. Senior Information Sharing and Safeguarding Steering Committee. 209
Sec. 4. Classified Information Sharing and Safeguarding Office. 210
Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks. 211
Sec. 6. Insider Threat Task Force. .................................... 212
Sec. 7. General Provisions. ............................................. 213

Implementation of the Executive Order, “Classified National Security
Information” .............................................................. 215
1. Initial Implementation Efforts. ...................................... 215
2. Declassification of Records of Permanent Historical Value. .... 216
3. Delegation of Original Classification Authority. ................ 216
4. Promotion of New Technologies to Support Declassification. .. 216
5. Publication. ............................................................ 217

Original Classification Authority ....................................... 218
TOP SECRET ............................................................. 218
SECRET .............................................................. 219

LEGISLATIVE AGENCY RULES ........................................ 221
CFR TITLE 28—JUDICIAL ADMINISTRATION ..................... 222
28 CFR PART 5—ADMINISTRATION AND ENFORCEMENT OF FOREIGN AGENTS
REGISTRATION ACT OF 1938, AS AMENDED .................. 222
28 CFR PART 10—REGISTRATION OF CERTAIN ORGANIZATIONS CARRYING ON
ACTIVITIES WITHIN THE UNITED STATES ..................... 244
V. Clerk’s Office ........................................................................................................... 1350
VI. Form and Filing of Applications for Court Orders .............................................. 1350
VII. Hearings ............................................................................................................... 1352
VIII. Orders ............................................................................................................... 1353
IX. Sequestration or Destruction .............................................................................. 1354
X. Appeals ................................................................................................................. 1354
Appendix to the FISA Court Rules: Procedures for Review of Petitions Filed Pursuant to Section 501(F) of the Foreign Intelligence Surveillance Court Act of 1978 .................. 1356

**Alien Terrorist Removal Court Rules** .................................................................. 1363
Rule 1: Name of Court .......................................................................................... 1363
Rule 2: Seal .............................................................................................................. 1363
Rule 3: Situs .............................................................................................................. 1363
Rule 4: Clerk ............................................................................................................ 1363
Rule 5: Application for Removal ............................................................................ 1364
Rule 6: Assignment of Cases .................................................................................. 1364
Rule 7: Service of an Order Granting an Application and Notice of a Removal Hearing .............................................................................................................. 1364
Rule 8: Interim Hearing .......................................................................................... 1365
Rule 9: Place of Conducting Removal Hearing ..................................................... 1365
Rule 10: Verbatim Record of Proceedings ............................................................. 1365
Rule 11: Motions ..................................................................................................... 1365
Rule 12: Subpoenas .................................................................................................. 1366
Rule 13: Classified Information ............................................................................... 1366
Rule 14: Removal Hearing Memorandum .............................................................. 1366
# Full Table of Contents

**Preface** .......................................................................................................................... 4  
**Summary of Contents** ...................................................................................................... 5  
**Chapter-Level Table of Contents** ...................................................................................... 7  
**Full Table of Contents** ...................................................................................................... 13  
**PRESIDENTIAL RULES** .................................................................................................. 57  
  Executive Order 10865. Safeguarding Classified Information Within Industry .......................... 58  
  Modification of Executive Order No. 10865 ......................................................................... 58  
  Executive Order 12139. Exercise of Certain Authority Respecting Electronic Surveillance ........ 63  
  Executive Order 12333. United States Intelligence Activities ............................................ 65  
  TABLE OF CONTENTS ......................................................................................................... 65  
  PART 1—GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS ............................................................................ 66  
  1.1 Goals .................................................................................................................................. 66  
  1.2 The National Security Council .......................................................................................... 67  
  1.3 Director of National Intelligence ...................................................................................... 68  
  1.4 The Intelligence Community ............................................................................................ 74  
  1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies .... 75  
  1.6 Heads of Elements of the Intelligence Community .......................................................... 77  
  1.7 Intelligence Community Elements ................................................................................... 78  
  1.8 The Department of State ................................................................................................... 82  
  1.9 The Department of the Treasury ...................................................................................... 83  
  1.10 The Department of Defense ............................................................................................. 83  
  1.11 The Department of Homeland Security ......................................................................... 84  
  1.12 The Department of Energy .............................................................................................. 85  
  1.13 The Federal Bureau of Investigation .............................................................................. 85  
  PART 2—CONDUCT OF INTELLIGENCE ACTIVITIES .................................................... 85  
  2.1 Need .................................................................................................................................... 85  
  2.2 Purpose ............................................................................................................................... 85  
  2.3 Collection of Information ................................................................................................. 86  
  2.4 Collection Techniques ...................................................................................................... 87  
  2.5 Attorney General Approval .............................................................................................. 88  
  2.6 Assistance to Law Enforcement and other Civil Authorities ........................................... 88  
  2.7 Contracting ....................................................................................................................... 89  
  2.8 Consistency With Other Laws ........................................................................................... 89
2.9 Undisclosed Participation in Organizations Within the United States 89
2.10 Human Experimentation 90
2.11 Prohibition on Assassination 90
2.12 Indirect Participation 90
2.13 Limitation on Covert Action 90

PART 3—GENERAL PROVISIONS 90
3.1 Congressional Oversight 90
3.2 Implementation 90
3.3 Procedures 91
3.4 References and Transition 91
3.5 Definitions 91
3.6 Revocation 94
3.7 General Provisions 94

Executive Order 12829. National Industrial Security Program 95
PART 1. ESTABLISHMENT AND POLICY 95
  Section 101. Establishment. 95
  Sec. 102. Policy Direction. 96
  Sec. 103. National Industrial Security Program Policy Advisory Committee. 97

PART 2. OPERATIONS 98
  Sec. 201. National Industrial Security Program Operating Manual. 98
  Sec. 202. Operational Oversight. 99
  Sec. 203. Implementation. 100

Executive Order 12937. Declassification of Selected Records Within National Archives of United States 103

Executive Order 12949. Foreign Intelligence Physical Searches 105

Executive Order 12951. Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems 107
  Section 1. Public Release of Historical Intelligence Imagery. 107
  Sec. 2. Review for Future Public Release of Intelligence Imagery. 107
  Sec. 3. General Provisions. 108
  Sec. 4. Definition. 108

Executive Order 12968. Access to Classified Information 109
PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS 109
  Section 1.1. Definitions. 109
  Sec. 1.2. Access to Classified Information. 111
  Sec. 1.3. Financial Disclosure. 112
  Sec. 1.4. Use of Automated Financial Record Data Bases. 113
  Sec. 1.5. Employee Education and Assistance. 113

PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE 114
  Sec. 2.1. Eligibility Determinations. 114
  Sec. 2.2. Level of Access Approval. 114
  Sec. 2.3. Temporary Access to Higher Levels. 115
  Sec. 2.4. Reciprocal Acceptance of Access Eligibility Determinations. 115
  Sec. 2.5. Specific Access Requirement. 116
  Sec. 2.6. Access by Non-United States Citizens. 116

PART 3—ACCESS ELIGIBILITY STANDARDS 117
  Sec. 3.1. Standards. 117
  Sec. 3.2. Basis for Eligibility Approval. 118
  Sec. 3.3. Special Circumstances. 118
  Sec. 3.4. Reinvestigation Requirements. 119
  Sec. 3.5. Continuous Evaluation. 119
(b) Anonymous, hypothetical, non-party and ex post facto review requests excluded.

_________  
(c) Fee. ________________________________________________  223
(d) Address. ________________________________________________  224
(e) Contents. ________________________________________________  224
(f) Certification. ________________________________________________  224
(g) Additional information. ________________________________________________  224
(h) Outcomes. ________________________________________________  225
(i) Time for response. ________________________________________________  225
(j) Written decisions only. ________________________________________________  225
(k) Effect of review letter. ________________________________________________  225
(l) Compliance. ________________________________________________  225
(m) Confidentiality. ________________________________________________  225

28 CFR Section 5.3: Filing of a registration statement.  226
28 CFR Section 5.4: Computation of time.  226
28 CFR Section 5.5: Registration fees.  226
28 CFR Section 5.100: Definition of terms.  228
28 CFR Section 5.200: Registration.  230
28 CFR Section 5.201: Exhibits.  230
28 CFR Section 5.202: Short form registration statement.  231
28 CFR Section 5.203: Supplemental statement.  232
28 CFR Section 5.204: Amendments.  233
28 CFR Section 5.205: Termination of registration.  233
28 CFR Section 5.206: Language and wording of registration statement.  234
28 CFR Section 5.207: Incorporation by reference.  234
28 CFR Section 5.208: Disclosure of foreign principals.  235
28 CFR Section 5.209: Information relating to employees.  235
28 CFR Section 5.210: Amount of detail required in information relating to registrant’s activities and expenditures.  235
28 CFR Section 5.211: Sixty-day period to be covered in initial statement.  235
28 CFR Section 5.300: Burden of establishing availability of exemption.  235
28 CFR Section 5.301: Exemption under section 3(a) of the Act.  236
28 CFR Section 5.302: Exemptions under sections 3(b) and (c) of the Act.  236
28 CFR Section 5.303: Exemption available to persons accredited to international organizations.  236
28 CFR Section 5.304: Exemptions under sections 3(d) and (e) of the Act.  236
28 CFR Section 5.305: Exemption under section 3(f) of the Act.  237
28 CFR Section 5.306: Exemption under section 3(g) of the Act.  237
28 CFR Section 5.307: Exemption under 3(h) of the Act.  238
28 CFR Section 5.400: Filing of informational materials.  238
28 CFR Section 5.402: Labeling informational materials.  239
28 CFR Section 5.500: Maintenance of books and records.  240
28 CFR Section 5.501: Inspection of books and records.  241
28 CFR Section 5.600: Public examination of records.  241
28 CFR Section 5.601: Copies of records and information available.  242
28 CFR Section 5.800: Ten-day filing requirement.  242
28 CFR Section 5.801: Activity beyond 10-day period.  242

28 CFR PART 10—REGISTRATION OF CERTAIN ORGANIZATIONS CARRYING ON ACTIVITIES WITHIN THE UNITED STATES ____________________________ 244
REGISTRATION STATEMENT  245
28 CFR Section 10.1: Form of registration statement.  245
28 CFR Section 10.2: Language of registration statement.  245
28 CFR Section 10.3: Effect of acceptance of registration statement.  245
28 CFR Section 10.4: Date of filing.  246

______________________________  
Page 18
28 CFR Section 10.5: Incorporation of papers previously filed. ........................................... 246
28 CFR Section 10.6: Necessity for further registration. ......................................................... 246
28 CFR Section 10.7: Cessation of activity. ................................................................. 246
Supplemental Registration Statement .............................................................................. 247
28 CFR Section 10.8: Information to be kept current. ......................................................... 247
28 CFR Section 10.9: Requirements for supplemental registration statement. ............. 247
Inspection of Registration Statement .............................................................................. 247
28 CFR Section 10.10: Public inspection. .......................................................................... 247
28 CFR PART 12—REGISTRATION OF CERTAIN PERSONS HAVING KNOWLEDGE OF
FOREIGN ESPIONAGE, COUNTERESPIONAGE, OR SABOTAGE MATTERS UNDER THE
ACT OF AUGUST 1, 1956 ........................................................................................................ 248
28 CFR Section 12.1: Definitions. .................................................................................. 249
28 CFR Section 12.2: Administration of act. ................................................................. 249
28 CFR Section 12.3: Prior registration with the Foreign Agents Registration Unit. ........ 249
28 CFR Section 12.4: Inquiries concerning application of act. ....................................... 250
28 CFR Section 12.20: Filing of registration statement. ................................................... 250
28 CFR Section 12.21: Time within which registration statement must be filed. .......... 250
28 CFR Section 12.22: Material contents of registration statement. ............................. 250
28 CFR Section 12.23: Deficient registration statement. ................................................. 251
28 CFR Section 12.24: Forms, ................................................................. 252
28 CFR Section 12.25: Amended registration statement. ................................................. 252
28 CFR Section 12.30: Burden of establishing availability of exemptions. .................... 253
28 CFR Section 12.40: Public examination. ................................................................. 253
28 CFR Section 12.41: Photocopies. ............................................................................. 253
28 CFR Section 12.70: Partial compliance not deemed compliance. .............................. 254
28 CFR PART 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION
----------------------------------
SUBPART A—Procedures for Disclosure of Records Under the Freedom of Information
Act .................................................................................................................................. 255
28 CFR Section 16.1: General provisions. .................................................................. 259
28 CFR Section 16.2: Public reading rooms. ................................................................. 259
28 CFR Section 16.3: Requirements for making requests. ............................................. 261
   (a) How made and addressed. ......................................................................................... 261
   (b) Description of records sought. ................................................................................... 261
   (c) Agreement to pay fees. ............................................................................................ 262
28 CFR Section 16.4: Responsibility for responding to requests. ..................................... 262
   (a) In general. ................................................................................................................ 262
   (b) Authority to grant or deny requests. ......................................................................... 262
   (c) Consultations and referrals. ..................................................................................... 262
   (d) Law enforcement information. ................................................................................ 263
   (e) Classified information. ............................................................................................ 263
   (f) Notice of referral. ....................................................................................................... 263
   (g) Timing of responses to consultations and referrals. ................................................. 263
   (h) Agreements regarding consultations and referrals. ............................................... 264
28 CFR Section 16.5: Timing of responses to requests. ..................................................... 264
   (a) In general. ................................................................................................................ 264
   (b) Multitrack processing. ............................................................................................. 264
   (c) Unusual circumstances. ........................................................................................... 264
   (d) Expedited processing. .............................................................................................. 264
28 CFR Section 16.6: Responses to requests. .................................................................... 266
   (a) Acknowledgements of requests. ................................................................................ 266
   (b) Grants of requests. .................................................................................................... 266
   (c) Adverse determinations of requests. ........................................................................ 266
28 CFR Section 16.7: Classified information. ................................................................... 267
28 CFR Section 16.8: Business information. ................................................................... 267

Page 19
(a) In general. .......................................................... 267
(b) Definitions. ........................................................ 267
(c) Designation of business information. ....................... 267
(d) Notice to submitters. ............................................. 267
(e) Where notice is required. ....................................... 268
(f) Opportunity to object to disclosure. .......................... 268
(g) Notice of intent to disclose. .................................... 268
(h) Exceptions to notice requirements. ............................ 269
(i) Notice of FOIA lawsuit. .......................................... 269
(j) Corresponding notice to requesters. ........................... 269
28 CFR Section 16.9: Appeals. ................................. 269
(a) Appeals of adverse determinations. .......................... 269
(b) Responses to appeals. ............................................ 270
(c) When appeal is required. ....................................... 270
28 CFR Section 16.10: Preservation of records. ............... 270
28 CFR Section 16.11: Fees. .......................................... 271
(a) In general. .......................................................... 271
(b) Definitions. ........................................................ 271
(c) Fees. .................................................................. 273
(d) Limitations on charging fees. ................................... 274
(e) Notice of anticipated fees in excess of $25.00. ............ 275
(f) Charges for other services. ...................................... 275
(g) Charging interest. ................................................ 275
(h) Aggregating requests. .......................................... 275
(i) Advance payments. .............................................. 275
(j) Other statutes specifically providing for fees. .............. 276
(k) Requirements for waiver or reduction of fees. .......... 276
28 CFR Section 16.12: Other rights and services. ............. 278
SUBPART B—Production or Disclosure in Federal and State Proceedings ............ 279
28 CFR Section 16.21: Purpose and scope. ..................... 279
28 CFR Section 16.22: General prohibition of production or disclosure in Federal and State proceedings in which the United States is not a party. ........... 280
28 CFR Section 16.23: General disclosure authority in Federal and State proceedings in which the United States is a party. .................................................. 280
28 CFR Section 16.24: Procedure in the event of a demand where disclosure is not otherwise authorized. ............... 281
28 CFR Section 16.25: Final action by the Deputy or Associate Attorney General. ............ 284
28 CFR Section 16.26: Considerations in determining whether production or disclosure should be made pursuant to a demand. ........................................... 284
28 CFR Section 16.27: Procedure in the event a department decision concerning a demand is not made prior to the time a response to the demand is required. ............. 286
28 CFR Section 16.28: Procedure in the event of an adverse ruling. ......................... 286
28 CFR Section 16.29: Delegation by Assistant Attorneys General. ...................... 286
Appendix to SUBPART B of Part 16—Redelegation of Authority to the Deputy Assistant Attorney General for Litigation, Antitrust Division, To Authorize Production or Disclosure of Material or Information .............................................. 288
SUBPART C—Production of FBI Identification Records in Response to Written Requests by Subjects Thereof ................................................................. 289
28 CFR Section 16.30: Purpose and scope. ..................... 289
28 CFR Section 16.31: Definition of identification record. ............. 289
28 CFR Section 16.32: Procedure to obtain an identification record. ...................... 289
28 CFR Section 16.33: Fee for production of identification record. ....................... 290
28 CFR Section 16.34: Procedure to obtain change, correction or updating of identification records. .................................................. 290
<table>
<thead>
<tr>
<th>CFR Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.71</td>
<td>Exemption of the Office of the Deputy Attorney General System—limited access.</td>
<td>307</td>
</tr>
<tr>
<td>16.72</td>
<td>Exemption of Office of the Associate Attorney General System—limited access.</td>
<td>309</td>
</tr>
<tr>
<td>16.73</td>
<td>Exemption of Office of Legal Policy System—limited access.</td>
<td>311</td>
</tr>
<tr>
<td>16.74</td>
<td>Exemption of National Security Division Systems—limited access.</td>
<td>315</td>
</tr>
<tr>
<td>16.76</td>
<td>Exemption of Justice Management Division.</td>
<td>321</td>
</tr>
<tr>
<td>16.77</td>
<td>Exemption of U.S. Trustee Program System—limited access.</td>
<td>324</td>
</tr>
<tr>
<td>16.78</td>
<td>Exemption of the Special Counsel for Immigration-Related, Unfair Employment Practices Systems.</td>
<td>326</td>
</tr>
<tr>
<td>16.79</td>
<td>Exemption of Pardon Attorney System.</td>
<td>326</td>
</tr>
<tr>
<td>16.80</td>
<td>Exemption of Office of Professional Responsibility System—limited access.</td>
<td>327</td>
</tr>
<tr>
<td>16.81</td>
<td>Exemption of United States Attorneys Systems—limited access.</td>
<td>329</td>
</tr>
<tr>
<td>16.82</td>
<td>Exemption of the National Drug Intelligence Center Data Base—limited access.</td>
<td>336</td>
</tr>
<tr>
<td>16.83</td>
<td>Exemption of the Executive Office for Immigration Review System—limited access.</td>
<td>338</td>
</tr>
<tr>
<td>16.84</td>
<td>Exemption of Immigration Appeals System.</td>
<td>340</td>
</tr>
<tr>
<td>16.85</td>
<td>Exemption of U.S. Parole Commission—limited access.</td>
<td>340</td>
</tr>
<tr>
<td>16.88</td>
<td>Exemption of Antitrust Division Systems—limited access.</td>
<td>342</td>
</tr>
<tr>
<td>16.89</td>
<td>Exemption of Civil Division Systems—limited access.</td>
<td>344</td>
</tr>
<tr>
<td>16.90</td>
<td>Exemption of Civil Rights Division Systems.</td>
<td>348</td>
</tr>
<tr>
<td>16.91</td>
<td>Exemption of Criminal Division Systems—limited access, as indicated.</td>
<td>350</td>
</tr>
<tr>
<td>16.92</td>
<td>Exemption of Environment and Natural Resources Division Systems—limited access.</td>
<td>371</td>
</tr>
<tr>
<td>16.93</td>
<td>Exemption of Tax Division Systems—limited access.</td>
<td>374</td>
</tr>
<tr>
<td>16.96</td>
<td>Exemption of Federal Bureau of Investigation Systems—limited access.</td>
<td>380</td>
</tr>
<tr>
<td>16.97</td>
<td>Exemption of Bureau of Prisons Systems—limited access.</td>
<td>399</td>
</tr>
<tr>
<td>16.98</td>
<td>Exemption of the Drug Enforcement Administration (DEA)—limited access.</td>
<td>411</td>
</tr>
<tr>
<td>16.99</td>
<td>Exemption of the Immigration and Naturalization Service Systems—limited access.</td>
<td>417</td>
</tr>
<tr>
<td>16.100</td>
<td>Exemption of Office of Justice Programs—limited access.</td>
<td>426</td>
</tr>
<tr>
<td>16.101</td>
<td>Exemption of U.S. Marshals Service Systems—limited access, as indicated.</td>
<td>427</td>
</tr>
<tr>
<td>16.102</td>
<td>Exemption of Drug Enforcement Administration and Immigration and Naturalization Service Joint System of Records.</td>
<td>441</td>
</tr>
<tr>
<td>16.103</td>
<td>Exemption of the INTERPOL-States National Central Bureau (INTERPOL-USNCB) System.</td>
<td>444</td>
</tr>
<tr>
<td>16.104</td>
<td>Exemption of Office of Special Counsel—Waco System.</td>
<td>445</td>
</tr>
<tr>
<td>16.105</td>
<td>Exemption of Foreign Terrorist Tracking Task Force System.</td>
<td>447</td>
</tr>
<tr>
<td>16.106</td>
<td>Exemption of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—Limited Access.</td>
<td>448</td>
</tr>
<tr>
<td>16.130</td>
<td>Exemption of Department of Justice Systems: Correspondence Management Systems for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).</td>
<td>455</td>
</tr>
</tbody>
</table>
28 CFR Section 16.131: Exemption of Department of Justice (DOJ)/Nationwide Joint
Automated Booking System (JABS), DOJ-005. ____________________________ 457
28 CFR Section 16.132: Exemption of Department of Justice System—Personnel
Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-
006. __________________________________________________________________ 459
28 CFR Section 16.133: Exemption of Department of Justice Regional Data Exchange
System (RDEX), DOJ-012. _______________________________________________ 461
28 CFR Section 16.200: Definitions. ________________________________________ 463
28 CFR Section 16.201: Voting by the Commissioners without joint deliberation. ____ 465
28 CFR Section 16.202: Open meetings. _____________________________________ 465
28 CFR Section 16.203: Closed meetings—Formal procedure. _________________ 465
   (a) 466
   (b) Public interest provision. ____________________________________________________________________________ 468
   (c) Nonpublic matter in announcements. __________________________________________________________________ 468
   (d) Voting and certification. ____________________________________________________________________________ 468
28 CFR Section 16.204: Public notice. ________________________________________ 469
   (a) Requirements. _______________________________________________________________________________________ 469
   (b) Time of notice. _______________________________________________________________________________________ 470
   (c) Amendments to notice. ______________________________________________________________________________ 470
28 CFR Section 16.205: Closed meetings—Informal procedures. ________________ 470
   (a) Finding. ___________________________________________________________________________________________ 470
   (b) Meetings to which applicable. _________________________________________________________________________ 471
   (c) Written record of action to close meeting. ________________________________________________________________ 472
   (d) Public notice. _______________________________________________________________________________________ 472
28 CFR Section 16.206: Transcripts, minutes, and miscellaneous documents concerning
Commission meetings. __________________________________________________ 472
28 CFR Section 16.207: Public access to nonexempt transcripts and minutes of closed
Commission meetings—Documents used at meetings—Record retention. ______ 473
   (a) Public access to records. ____________________________________________________________________________ 473
   (b) Access to documents identified or discussed in any Commission meeting, open or
closed, shall be governed by Department of Justice regulations at this part 16, subparts
C and D. __________________________________________________________________________________________ 473
   (c) Retention of records. ________________________________________________________________________________ 474
28 CFR Section 16.208: Annual report. ________________________________________ 474
SUBPART G—Access to Documents by Former Employees of the Department ______ 475
28 CFR Section 16.300: Access to documents for the purpose of responding to an official
inquiry. ________________________________________________________________________________________________ 475
28 CFR Section 16.301: Limitations. __________________________________________ 475
APPENDIX I TO PART 16—COMPONENTS OF THE DEPARTMENT OF JUSTICE 477
28 CFR PART 17—CLASSIFIED NATIONAL SECURITY INFORMATION AND ACCESS TO
CLASSIFIED INFORMATION ____________________________________________ 480
28 CFR Section 17.1: Purpose. _____________________________________________ 482
28 CFR Section 17.2: Scope. ______________________________________________ 483
28 CFR Section 17.3: Definitions. __________________________________________ 483
SUBPART A—Administration _______________________________________________ 484
28 CFR Section 17.11: Authority of the Assistant Attorney General for Administration. 484
28 CFR Section 17.12: Component head responsibilities. ______________________ 486
28 CFR Section 17.13: National Security Division; interpretation of Executive Orders. 486
28 CFR Section 17.14: Department Review Committee. ________________________ 487
28 CFR Section 17.15: Access Review Committee. ____________________________ 488
28 CFR Section 17.16: Violations of classified information requirements. ________ 489
28 CFR Section 17.17: Judicial proceedings. ________________________ 489
28 CFR Section 17.18: Prepublication review. ________________________________ 491
SUBPART B—Classified Information _________________________________________ 495
(g) Access and review.  
28 CFR Section 20.23: Documentation: Approval by OJARS.  
28 CFR Section 20.24: State laws on privacy and security.  
28 CFR Section 20.25: Penalties.  

SUBPART C—Federal Systems and Exchange of Criminal History Record Information  
28 CFR Section 20.30: Applicability.  
28 CFR Section 20.31: Responsibilities.  
28 CFR Section 20.32: Includable offenses.  
28 CFR Section 20.33: Dissemination of criminal history record information.  
28 CFR Section 20.34: Individual’s right to access criminal history record information.  
28 CFR Section 20.35: Criminal Justice Information Services Advisory Policy Board.  
28 CFR Section 20.36: Participation in the Interstate Identification Index System.  
28 CFR Section 20.38: Sanction for noncompliance.  
Appendix to Part 20—Commentary on Selected Sections of the Regulations on Criminal History Record Information Systems  
Subpart A  
Subpart B  
Subpart C  

28 CFR PART 21—WITNESS FEES  
28 CFR Section 21.1: Definitions.  
(a) Agency proceeding.  
(b) Alien.  
(c) Judicial proceeding.  
(d) Pre-trial conference.  
(e) Residence.  
(f) Summons.  
28 CFR Section 21.2: Employees of the United States serving as witnesses.  
(a) Applicability.  
(b) Entitlement to travel expenses  
(c) Allowable travel expenses.  
(d) Payment and reimbursement  
(e) Leave and attendance fee  
28 CFR Section 21.3: Aliens.  
(a) Aliens entitled to payment of $30 per day.  
(b) Aliens entitled to payment of $1 per day.  
(c) Aliens not entitled to payment.  
(d) Doubtful cases.  
28 CFR Section 21.4: Fees and allowances of fact witnesses.  
(a) Fee.  
(b) Allowable transportation expenses.  
(c) Subsistence allowance.  
(d) Detained witness fee.  
28 CFR Section 21.5: Use of table of distances.  
(a) Civil cases.  
(b) Criminal cases.  
28 CFR Section 21.7: Certification of witness attendance.  

28 CFR PART 22—CONFIDENTIALITY OF IDENTIFIABLE RESEARCH AND STATISTICAL INFORMATION  
28 CFR Section 22.1: Purpose.  
28 CFR Section 22.2: Definitions.  

28 CFR Section 24.305: Extensions of time. .................................................. 575
28 CFR Section 24.306: Decision on application. ..................................... 575
28 CFR Section 24.307: Department review. ............................................. 576
28 CFR Section 24.308: Judicial review. ...................................................... 576
28 CFR Section 24.309: Payment of award. ............................................... 576
28 CFR PART 25—DEPARTMENT OF JUSTICE INFORMATION SYSTEMS 577
SUBPART A—The National Instant Criminal Background Check System 578
28 CFR Section 25.1: Purpose and authority. ............................................. 578
28 CFR Section 25.2: Definitions. ............................................................... 578
Appeal ......................................... 578
ARI ............................................. 578
ATF ............................................. 578
Audit log .......................................... 578
Business day ..................................... 578
Control Terminal Agency ................................................................. 579
Data source ........................................ 579
Delayed ........................................... 579
Denied ............................................. 579
Denying agency .................................... 579
Dial-up access ..................................... 579
Federal agency ..................................... 579
FFL (federal firearms licensee) ......................................................... 579
Firearm ........................................... 580
Licensed dealer ...................................... 580
Licensed importer ...................................... 580
Licensed manufacturer ..................................... 580
NCIC (National Crime Information Center) ........................................... 580
NICS ............................................ 580
NICS Index ......................................... 580
NICS operational day ........................................ 580
NICS Representative ...................................... 580
NRI (NICS Record Identifier) ......................................................... 581
NTN (NICS Transaction Number) ..................................................... 581
Open ............................................... 581
ORI (Originating Agency Identifier) ..................................................... 581
Originating Agency .......................................... 581
POC (Point of Contact) ............................................................ 581
Proceed ............................................ 582
Record ............................................... 582
STN (State-Assigned Transaction Number) ........................................... 582
System ................................................ 582
28 CFR Section 25.3: System information. ............................................. 582
28 CFR Section 25.4: Record source categories. ..................................... 583
28 CFR Section 25.5: Validation and data integrity of records in the system. 583
28 CFR Section 25.6: Accessing records in the system. ............................. 583
(a) .................................................. 583
(b) Access to the NICS through the FBI NICS Operations Center. .......... 584
(c) .................................................. 584
(d) Access to the NICS through POCs. ............................................... 585
(e) .................................................. 585
(f) .................................................. 585
(g) .................................................. 586
(h) POC Determination Messages. ..................................................... 586
(i) Response recording. .............................................................. 586
(j) Access to the NICS Index for purposes unrelated to NICS background checks required by the Brady Act.

28 CFR Section 25.7: Querying records in the system. ......................................................... 587
28 CFR Section 25.8: System safeguards. ........................................................................... 588
28 CFR Section 25.9: Retention and destruction of records in the system. ....................... 590
28 CFR Section 25.10: Correction of erroneous system information. ............................. 593
28 CFR Section 25.11: Prohibited activities and penalties. ............................................. 595

SUBPART B—National Motor Vehicle Title Information System (NMVTIS) ................. 596
28 CFR Section 25.51: Purpose and authority. ................................................................. 596
28 CFR Section 25.52: Definitions. ................................................................................... 596

Acquiring .................................................................................................................. 596
Automobile ............................................................................................................... 596
Certificate of title .................................................................................................... 596
Insurance carrier .................................................................................................... 596
Junk automobile ...................................................................................................... 596
Junk yard .................................................................................................................. 597
Motor vehicle .......................................................................................................... 597
NMVTIS .................................................................................................................. 597
Operator .................................................................................................................... 597
Purchaser .................................................................................................................. 597
Salvage automobile ................................................................................................ 597
Salvage yard ............................................................................................................. 597
State .......................................................................................................................... 598
Total loss .................................................................................................................... 598
VIN .............................................................................................................................. 598

28 CFR Section 25.53: Responsibilities of the operator of NMVTIS. ............................ 598
28 CFR Section 25.54: Responsibilities of the States. .................................................... 600
28 CFR Section 25.55: Responsibilities of insurance carriers. ...................................... 602
28 CFR Section 25.56: Responsibilities of junk yards and salvage yards and auto recyclers. .......................................................... 603
28 CFR Section 25.57: Erroneous junk or salvage reporting. ......................................... 604

28 CFR PART 27—WHISTLEBLOWER PROTECTION FOR FEDERAL BUREAU OF INVESTIGATION EMPLOYEES ................................................................. 606
SUBPART A—Protected Disclosures of Information ....................................................... 607
28 CFR Section 27.1: Making a protected disclosure. ................................................... 607
28 CFR Section 27.2: Prohibition against reprisal for making a protected disclosure. ......... 607

SUBPART B—Investigating Reprisal Allegations and Ordering Corrective Action .......... 609
28 CFR Section 27.4: Corrective action and other relief; Director, Office of Attorney
Recruitment and Management. ................................................................................... 610
28 CFR Section 27.5: Review. ....................................................................................... 613
28 CFR Section 27.6: Extensions of time. ................................................................. 613

28 CFR PART 28—DNA IDENTIFICATION SYSTEM ........................................................................ 614
SUBPART A—Qualifying Federal Offenses for Purposes of DNA Sample Collection .... 615
28 CFR Section 28.1: Purpose. .................................................................................... 615
28 CFR Section 28.2: Determination of offenses. ........................................................ 615
(a) Felony ................................................................................................................... 615

SUBPART B—DNA Sample Collection, Analysis, and Indexing ........................................ 617
28 CFR Section 28.11: Definitions. ............................................................................. 617
DNA analysis ........................................................................................................... 617
DNA sample ............................................................................................................ 617
28 CFR Section 28.12: Collection of DNA samples. ....................................................... 617
28 CFR Section 28.13: Analysis and indexing of DNA samples. ................................... 619

SUBPART C—Preservation of Biological Evidence .......................................................... 620
28 CFR Section 28.21: Purpose. ____________________________________________ 620
28 CFR Section 28.22: The requirement to preserve biological evidence. __________________________ 620
   (a) Applicability in general. ____________________________________________ 620
   (b) Limitation to circumstances in which a defendant is under a sentence of
       imprisonment for the offense. ____________________________________________ 620
   (c) Conditions of preservation. ____________________________________________ 621
28 CFR Section 28.23: Evidence subject to the preservation requirement. ____________________________ 621
   (a) Biological evidence generally. ____________________________________________ 621
   (b) Biological evidence under section 3600A(b)(2). ____________________________ 621
28 CFR Section 28.24: Exceptions based on the results of judicial proceedings. ____________________________ 623
   (a) Judicial denial of DNA testing. ____________________________________________ 623
   (b) Inclusion of defendant as source. ____________________________________________ 623
28 CFR Section 28.25: Exceptions based on a defendant's conduct. ____________________________ 623
   (a) Waiver by defendant. ____________________________________________ 623
   (b) Notice to defendant. ____________________________________________ 623
28 CFR Section 28.26: Exceptions based on the nature of the evidence. ____________________________ 624
   (a) Evidence not retained beyond the investigative stage. ____________________________ 624
   (b) Evidence not constituting biological material. ____________________________ 625
   (c) Preservation of portions sufficient for DNA testing. ____________________________ 625
28 CFR Section 28.27: Non-preemption of other requirements. ____________________________ 626
28 CFR Section 28.28: Sanctions for violations. ____________________________ 626
   (a) Disciplinary sanctions. ____________________________________________ 626
   (b) Criminal sanctions. ____________________________________________ 626
   (c) No effect on validity of convictions. ____________________________________________ 626

28 CFR PART 29—MOTOR VEHICLE THEFT PREVENTION ACT REGULATIONS __________ 627
28 CFR Section 29.1: Purpose. ____________________________________________ 628
28 CFR Section 29.2: Definitions. ____________________________________________ 628
   (a) The Act ____________________________________________ 628
   (b) Owner ____________________________________________ 628
   (c) The Program ____________________________________________ 628
28 CFR Section 29.3: Administration by the Bureau of Justice Assistance. ____________________________ 629
28 CFR Section 29.4: Election to participate by states and localities. ____________________________ 629
28 CFR Section 29.5: Notification of law enforcement officials. ____________________________ 629
28 CFR Section 29.6: Limited participation by states and localities permitted. ____________________________ 630
28 CFR Section 29.7: Withdrawal from the program by states and localities. ____________________________ 630
28 CFR Section 29.8: Motor vehicle owner participation. ____________________________ 630
28 CFR Section 29.9: Motor vehicles for hire. ____________________________ 631
28 CFR Section 29.10: Owner withdrawal from the program. ____________________________ 631
28 CFR Section 29.11: Sale or other transfer of an enrolled vehicle. ____________________________ 631
28 CFR Section 29.12: Specified conditions under which stops may be authorized. ____________________________ 631
   (a) Time. ____________________________________________ 631
   (b) Border crossing or port entry. ____________________________________________ 632
28 CFR Section 29.13: No new conditions without consent. ____________________________ 632

28 CFR PART 45—EMPLOYEE RESPONSIBILITIES __________ 633
28 CFR Section 45.1: Cross-reference to ethical standards and financial disclosure regulations. ____________________________ 634
28 CFR Section 45.2: Disqualification arising from personal or political relationship. ____________________________ 634
28 CFR Section 45.3: Disciplinary proceedings under 18 U.S.C. 207(j). ____________________________ 635
28 CFR Section 45.4: Personal use of Government property. ____________________________ 638
28 CFR Section 45.10: Procedures to promote compliance with crime victims' rights obligations. ____________________________ 638
   (a) Definitions. ____________________________________________ 638
   (b) ____________________________________________ 639
   (c) Complaint process. ____________________________________________ 639
   (d) ____________________________________________ 641
(a) General. .................................................................................. 669
(b) Guidelines to criminal actions. .................................................... 669
(c) Guidelines to civil actions. .......................................................... 671
28 CFR Section 50.3: Guidelines for the enforcement of title VI, Civil Rights Act of 1964. 
......................................................................................................... 672
28 CFR Section 50.5: Notification of Consular Officers upon the arrest of foreign 
nationals. ........................................................................................ 677
28 CFR Section 50.6: Antitrust Division business review procedure. .......... 678
28 CFR Section 50.7: Consent judgments in actions to enjoin discharges of pollutants. 
......................................................................................................... 681
28 CFR Section 50.8: [Reserved] .......................................................... 682
28 CFR Section 50.9: Policy with regard to open judicial proceedings. .......... 682
28 CFR Section 50.10: Policy with regard to the issuance of subpoenas to members of the 
news media, subpoenas for telephone toll records of members of the news media, and the 
interrogation, indictment, or arrest of, members of the news media. ........... 684
28 CFR Section 50.12: Exchange of FBI identification records. .................. 688
28 CFR Section 50.14: Guidelines on employee selection procedures. ........... 689
28 CFR Section 50.15: Representation of Federal officials and employees by Department 
of Justice attorneys or by private counsel furnished by the Department in civil, criminal, 
and congressional proceedings in which Federal employees are sued, subpoenaed, or 
charged in their individual capacities. ................................................ 735
28 CFR Section 50.16: Representation of Federal employees by private counsel at Federal 
expense. ............................................................................................ 741
28 CFR Section 50.17: Ex parte communications in informal rulemaking proceedings. 
.......................................................... 742
28 CFR Section 50.18: [Reserved] .......................................................... 743
28 CFR Section 50.19: Procedures to be followed by government attorneys prior to filing 
recusal or disqualification motions. ................................................... 743
28 CFR Section 50.20: Participation by the United States in court-annexed arbitration. 
......................................................................................................... 744
(a) Considerations affecting participation in arbitration. ......................... 745
(b) General rule consenting to arbitration consistent with the department's 
regulations. .................................................................................... 745
(c) Objection to the imposition of penalties or sanctions against the United States for 
demanding trial de novo. ........................................................... 746
(d) Additional restrictions. .................................................................. 747
(e) Notification of new or revised arbitration rules. .................................. 748
28 CFR Section 50.21: Procedures governing the destruction of contraband drug 
evidence in the custody of Federal law enforcement authorities. .............. 748
(a) General. .................................................................................. 748
(b) Purpose. .................................................................................. 749
(c) Policy. ..................................................................................... 749
(d) Definitions. ................................................................................ 749
(e) Procedures. ................................................................................ 750
(f) Procedures. ................................................................................ 751
(g) Supplementary regulations. ........................................................... 752
28 CFR Section 50.22: Young American Medals Program. ........................ 752
(a) Scope. ..................................................................................... 752
(b) Young American Medal for Bravery. .............................................. 752
(c) Young American Medal for Service. .............................................. 753
(d) Eligibility. .................................................................................. 753
(e) Request for information. ............................................................. 753
(f) Procedure. .................................................................................. 754
(g) Presentation. ................................................................................ 755
(h) Posthumous awards. ....................................................................... 755
(i) Young American Medals Committee. ............................................. 756

Page 31
28 CFR Section 50.23: Policy against entering into final settlement agreements or consent decree that are subject to confidentiality provisions and against seeking or concurring in the sealing of such documents. 756
28 CFR Section 50.24: Annuity broker minimum qualifications. 757
(a) Minimum standards. 757
(b) Procedures for inclusion on the list. 758
(c) Disclaimers. 759
28 CFR PART 52—PROCEEDINGS BEFORE U.S. MAGISTRATE JUDGES 761
28 CFR Section 52.01: Civil proceedings: Special master, pretrial, trial, appeal. 761
28 CFR Section 52.02: Criminal proceedings: Pretrial, trial. 762
28 CFR PART 59—GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES 764
28 CFR Section 59.1: Introduction. 764
28 CFR Section 59.2: Definitions. 765
28 CFR Section 59.3: Applicability. 765
28 CFR Section 59.4: Procedures. 766
(a) Provisions governing the use of search warrants generally. 767
(b) Provisions governing the use of search warrants which may intrude upon professional, confidential relationships. 767
(c) Considerations bearing on choice of methods. 769
28 CFR Section 59.5: Functions and authorities of the Deputy Assistant Attorneys General. 771
28 CFR Section 59.6: Sanctions. 771
28 CFR PART 60—AUTHORIZATION OF FEDERAL LAW ENFORCEMENT OFFICERS TO REQUEST THE ISSUANCE OF A SEARCH WARRANT 772
28 CFR Section 60.1: Purpose. 772
28 CFR Section 60.2: Authorized categories. 772
28 CFR Section 60.3: Agencies with authorized personnel. 774
(a) National Law Enforcement Agencies: 774
(b) Local Law Enforcement Agencies: 775
28 CFR PART 65—EMERGENCY FEDERAL LAW ENFORCEMENT ASSISTANCE 777
SUBPART A—Eligible Applicants 779
28 CFR Section 65.1: General. 779
28 CFR Section 65.2: State Government. 779
SUBPART B—Allocation of Funds and Other Assistance 779
28 CFR Section 65.10: Fund availability. 779
28 CFR Section 65.11: Limitations on fund and other assistance use. 779
(a) Land acquisition. 779
(b) Non-supplantation. 779
(c) Civil justice. 779
(d) Federal law enforcement personnel. 780
(e) Direction, supervision, control. 780
28 CFR Section 65.12: Other assistance. 780
SUBPART C—Purpose of Emergency Federal Law Enforcement Assistance 781
28 CFR Section 65.20: General. 781
28 CFR Section 65.21: Purpose of assistance. 781
28 CFR Section 65.22: Exclusions. 781
SUBPART D—Application for Assistance 782
28 CFR Section 65.30: General. 782
28 CFR Section 65.31: Application content. 782
(a) Problem. 782
(b) Cause. 782
(c) Resources. 782
(d) Assistance requested. 782
(e) Other assistance. 782

Page 32
28 CFR Section 69.200: Agency and legislative liaison. ........................................ 804
28 CFR Section 69.205: Professional and technical services. .......................... 804
28 CFR Section 69.210: Reporting. ................................................................ 805
SUBPART C—Activities by Other Than Own Employees ................................ 807
28 CFR Section 69.300: Professional and technical services. ......................... 807
SUBPART D—Penalties and Enforcement .......................................................... 809
28 CFR Section 69.400: Penalties. .................................................................. 809
28 CFR Section 69.405: Penalty procedures. ................................................... 809
28 CFR Section 69.410: Enforcement. ............................................................... 810
SUBPART E—Exemptions .................................................................................. 811
28 CFR Section 69.500: Secretary of Defense. .................................................. 811
SUBPART F—Agency Reports ......................................................................... 812
28 CFR Section 69.600: Semi-annual compilation. ........................................... 812
28 CFR Section 69.605: Inspector General report. ............................................ 813
Appendix A to Part 69—Certification Regarding Lobbying ............................... 814
Certification for Contracts, Grants, Loans, and Cooperative Agreements ........ 814
Statement for Loan Guarantees and Loan Insurance ........................................ 814
Appendix B to Part 69—Disclosure Form To Report Lobbying ...................... 816
28 CFR PART 73—NOTIFICATIONS TO THE ATTORNEY GENERAL BY AGENTS OF
FOREIGN GOVERNMENTS ......................................................................... 817
28 CFR Section 73.1: Definition of terms. .......................................................... 818
28 CFR Section 73.2: Exceptions. ................................................................... 819
28 CFR Section 73.3: Form of notification. ....................................................... 819
28 CFR Section 73.4: Partial compliance not deemed compliance. .................. 820
28 CFR Section 73.5: Termination of notification. ............................................. 820
28 CFR Section 73.6: Relation to other statutes. .............................................. 821
28 CFR PART 77—ETHICAL STANDARDS FOR ATTORNEYS FOR THE GOVERNMENT
.......................................................... .......................... .......................... 822
28 CFR Section 77.1: Purpose and authority. ..................................................... 823
28 CFR Section 77.2: Definitions. ................................................................... 823
28 CFR Section 77.3: Application of 28 U.S.C. 530B. ....................................... 825
28 CFR Section 77.4: Guidance. .................................................................... 826
(a) Rules of the court before which a case is pending. .................................... 826
(b) Inconsistent rules where there is a pending case. ...................................... 826
(c) Choice of rules where there is no pending case. ........................................ 826
(d) Rules that impose an irreconcilable conflict. ............................................ 826
(e) Supervisory attorneys. ............................................................................. 827
(f) Investigative Agents. ................................................................................ 827
28 CFR Section 77.5: No private remedies. ..................................................... 827
28 CFR PART 80—FOREIGN CORRUPT PRACTICES ACT OPINION PROCEDURE 828
28 CFR Section 80.1: Purpose. ...................................................................... 829
28 CFR Section 80.2: Submission requirements. ............................................. 829
28 CFR Section 80.3: Transaction. ................................................................. 829
28 CFR Section 80.4: Issuer or domestic concern. .......................................... 829
28 CFR Section 80.5: Affected parties. ............................................................ 829
28 CFR Section 80.6: General requirements. ................................................. 830
28 CFR Section 80.7: Additional information. ................................................. 830
28 CFR Section 80.8: Attorney General opinion. .......................................... 831
28 CFR Section 80.9: No oral opinion. ............................................................ 831
28 CFR Section 80.10: Rebuttable presumption. ............................................ 831
28 CFR Section 80.11: Effect of FCPA Opinion. ............................................. 831
28 CFR Section 80.12: Accounting requirements. .......................................... 832
28 CFR Section 80.13: Scope of FCPA Opinion. ............................................. 832
28 CFR Section 80.14: Disclosure. ................................................................. 832
28 CFR Section 80.15: Withdrawal. ................................................................. 833

Page 34
(d) Records.

28 CFR Section 105.13: Notification for candidates not eligible for expedited processing.

28 CFR Section 105.14: Risk assessment for candidates.

SUBPART C—Private Security Officer Employment

28 CFR Section 105.21: Purpose and authority.

28 CFR Section 105.22: Definitions.

(a) Authorized employer

(b) Employee

(c) Charged

(d) Felony

(e) Participating State

(f) Person

(g) Private Security Officer

(h) Security services

(i) State Identification Bureau (SIB)

28 CFR Section 105.23: Procedure for requesting criminal history record check.

28 CFR Section 105.24: Employee’s rights.

28 CFR Section 105.25: Authorized employer’s responsibilities.

28 CFR Section 105.26: State agency’s responsibilities.

28 CFR Section 105.27: Miscellaneous provisions.

(a) Alternate State availability.

(b) FBI fees for national check.

(c) Penalties for misuse.

(d) Exclusion from coverage.

28 CFR PART 200—ALIEN TERRORIST REMOVAL PROCEDURES

28 CFR Section 200.1: Eligibility for Protection under the Convention Against Torture.

CFR TITLE 32—NATIONAL DEFENSE

32 CFR CHAPTER XVII—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

32 CFR PART 1700—PROCEDURES FOR DISCLOSURE OF RECORDS PURSUANT TO THE FREEDOM OF INFORMATION ACT

32 CFR Section 1700.1: Purpose, scope, applicability.

32 CFR Section 1700.2: Definitions.

32 CFR Section 1700.3: Contact for general information and requests.

32 CFR Section 1700.4: Preliminary information.

32 CFR Section 1700.5: Requirements as to form and content.

32 CFR Section 1700.6: Fees for records services.

32 CFR Section 1700.7: Processing of requests for records.

32 CFR Section 1700.8: Action on the request.

32 CFR Section 1700.9: Payment of fees, notification of decision, and right of appeal.

32 CFR Section 1700.10: Procedures for business information.

32 CFR Section 1700.11: Procedures for information concerning other persons.

32 CFR Section 1700.12: Requests for expedited processing.

32 CFR Section 1700.13: Right to appeal and appeal procedures.

32 CFR Section 1700.14: Action by appeals authority.

32 CFR PART 1701—ADMINISTRATION OF RECORDS UNDER THE PRIVACY ACT OF 1974

SUBPART A—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974

32 CFR Section 1701.1: Purpose, scope, applicability.

32 CFR Section 1701.2: Definitions.

32 CFR Section 1701.3: Contact for general information and requests.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1701.4</td>
<td>Privacy Act responsibilities/policy.</td>
<td>891</td>
</tr>
<tr>
<td>1701.5</td>
<td>Collection and maintenance of records.</td>
<td>891</td>
</tr>
<tr>
<td>1701.6</td>
<td>Disclosure of records/policy.</td>
<td>892</td>
</tr>
<tr>
<td>1701.7</td>
<td>Requests for notification of and access to records.</td>
<td>893</td>
</tr>
<tr>
<td>1701.8</td>
<td>Requests to amend or correct records.</td>
<td>894</td>
</tr>
<tr>
<td>1701.9</td>
<td>Requests for an accounting of record disclosures.</td>
<td>895</td>
</tr>
<tr>
<td>1701.10</td>
<td>ODNI responsibility for responding to access requests.</td>
<td>895</td>
</tr>
<tr>
<td>1701.11</td>
<td>ODNI responsibility for responding to requests for amendment or correction.</td>
<td>897</td>
</tr>
<tr>
<td>1701.12</td>
<td>ODNI responsibility for responding to requests for accounting.</td>
<td>898</td>
</tr>
<tr>
<td>1701.13</td>
<td>Special procedures for medical/psychiatric/psychological records.</td>
<td>899</td>
</tr>
<tr>
<td>1701.14</td>
<td>Appeals.</td>
<td>899</td>
</tr>
<tr>
<td>1701.15</td>
<td>Fees.</td>
<td>900</td>
</tr>
<tr>
<td>1701.16</td>
<td>Contractors.</td>
<td>900</td>
</tr>
<tr>
<td>1701.17</td>
<td>Standards of conduct.</td>
<td>900</td>
</tr>
<tr>
<td>1701.20</td>
<td>Exemption policies.</td>
<td>902</td>
</tr>
<tr>
<td>1701.21</td>
<td>Exemption of National Counterterrorism Center (NCTC) systems of records.</td>
<td>902</td>
</tr>
<tr>
<td>1701.22</td>
<td>Exemption of Office of the National Counterintelligence Executive (ONCIX) system of records.</td>
<td>906</td>
</tr>
<tr>
<td>1701.23</td>
<td>Exemption of Office of Inspector General (OIG) systems of records.</td>
<td>908</td>
</tr>
<tr>
<td>1701.24</td>
<td>Exemption of Office of the Director of National Intelligence (ODNI) systems of records.</td>
<td>912</td>
</tr>
</tbody>
</table>

**SUBPART B—Exemption of Record Systems under the Privacy Act**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1701.20</td>
<td>Exemption policies.</td>
<td>902</td>
</tr>
<tr>
<td>1701.21</td>
<td>Exemption of National Counterterrorism Center (NCTC) systems of records.</td>
<td>902</td>
</tr>
<tr>
<td>1701.22</td>
<td>Exemption of Office of the National Counterintelligence Executive (ONCIX) system of records.</td>
<td>906</td>
</tr>
<tr>
<td>1701.23</td>
<td>Exemption of Office of Inspector General (OIG) systems of records.</td>
<td>908</td>
</tr>
</tbody>
</table>

**SUBPART C—Routine Uses Applicable to More Than One ODNI System of Records**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1701.30</td>
<td>Policy and applicability.</td>
<td>914</td>
</tr>
<tr>
<td>1701.31</td>
<td>General routine uses.</td>
<td>914</td>
</tr>
</tbody>
</table>

**SUBPART A—General**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800.1</td>
<td>Authority and purpose.</td>
<td>926</td>
</tr>
<tr>
<td>1800.2</td>
<td>Definitions.</td>
<td>926</td>
</tr>
<tr>
<td>1800.3</td>
<td>Contact for general information and requests.</td>
<td>929</td>
</tr>
<tr>
<td>1800.4</td>
<td>Suggestions and complaints.</td>
<td>929</td>
</tr>
</tbody>
</table>

**SUBPART B—Filing of FOIA Requests**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800.11</td>
<td>Preliminary information.</td>
<td>931</td>
</tr>
</tbody>
</table>
TIVE ORDER 12958

AUTHORIZED HOLDERS PURSUANT TO SECTION 1.9 OF EXECU
32 CFR PART 1802

32 CFR Section 1801.63: Specific
SUBPART G
32 CFR Section 1801.52: Criminal penalties.
32 CFR Section 1801.51: Limitations on disclosure.
SUBPART F
32 CFR Section 1801.45: Notification of decision and right of judicial review.
32 CFR Section 1801.44: Action by appeals authority.
32 CFR Section 1801.43: Determination(s) by Office Chiefs.
32 CFR Section 1801.42: Right of appeal and appeal procedures.
32 CFR Section 1801.41: Appeal authority.
SUBPART E
32 CFR Section 1801.34: Requests for expedited processing.
32 CFR Section 1801.33: Allocation of resources; agreed extensions of time.
32 CFR Section 1801.32: Requests for expedited processing.
32 CFR Section 1801.31: Procedures for business information.
32 CFR Section 1801.30: Procedures for information concerning other persons.
32 CFR Section 1801.29: Action and determination(s) by originator(s) or any interested party.
32 CFR Section 1801.28: Payment of fees, notification of decision, and right of appeal.
SUBPART D—Additional Administrative Matters
32 CFR Section 1801.27: Action On Privacy Act Administrative Appeals
32 CFR Section 1801.26: Payment of fees for record services.
32 CFR Section 1801.25: Payment of fees for record services.
32 CFR Section 1801.24: Requests for expedited processing.
32 CFR Section 1801.23: Payment of fees, notification of decision, and right of appeal.
SUBPART C
32 CFR Section 1801.22: Action and determination(s) by originator(s) or any interested party.
32 CFR Section 1801.21: Processing requests for access to or amendment of records.
32 CFR Section 1801.20: Action and determination(s) by originator(s) or any interested party.
32 CFR Section 1801.19: Payment of fees, notification of decision, and right of appeal.
SUBPART B
32 CFR Section 1801.18: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.17: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.16: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.15: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.14: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.13: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.12: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.11: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.10: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.9: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.8: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.7: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.6: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.5: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.4: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.3: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.2: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974
32 CFR Section 1801.1: APPLICABLE RIGHTS UNDER THE PRIVACY ACT OF 1974

Page 38
SUBPART A—General
32 CFR Section 1802.1: Authority and purpose.
32 CFR Section 1802.2: Definitions.
32 CFR Section 1802.3: Contact for general information and requests.
32 CFR Section 1802.4: Suggestions and complaints.

SUBPART B—Filing Of Challenges
32 CFR Section 1802.11: Prerequisites.
32 CFR Section 1802.12: Requirements as to form.
32 CFR Section 1802.13: Identification of material at issue.
32 CFR Section 1802.14: Transmission.

SUBPART C—Action On Challenges
32 CFR Section 1802.21: Receipt, recording, and tasking.
32 CFR Section 1802.22: Challenges barred by res judicata.
32 CFR Section 1802.23: Response by originator(s) and/or any interested party.
32 CFR Section 1802.24: Designation of authority to hear challenges.
32 CFR Section 1802.25: Action on challenge.
32 CFR Section 1802.26: Notification of decision and prohibition on adverse action.

SUBPART D—Right of Appeal
32 CFR Section 1802.31: Right of appeal.

SUBPART E—Further Appeals
32 CFR Section 1802.41: Right of further appeal.

32 CFR PART 1803—PUBLIC REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW OF CLASSIFIED INFORMATION PURSUANT TO SECTION 3.6 OF EXECUTIVE ORDER 12958

SUBPART A—General
32 CFR Section 1803.1: Authority and purpose.
32 CFR Section 1803.2: Definitions.
32 CFR Section 1803.3: Contact for general information and requests.
32 CFR Section 1803.4: Suggestions and complaints.

SUBPART B—Filing of Mandatory Declassification Review (MDR) Requests
32 CFR Section 1803.11: Preliminary information.
32 CFR Section 1803.12: Requirements as to form.
32 CFR Section 1803.13: Fees.

SUBPART C—NACIC Action on MDR Requests
32 CFR Section 1803.21: Receipt, recording, and tasking.
32 CFR Section 1803.22: Challenges barred by res judicata.
32 CFR Section 1803.23: Determination by originator or interested party.
32 CFR Section 1803.24: Notification of decision and right of appeal.

SUBPART D—NACIC Action on MDR Appeals
32 CFR Section 1803.31: Requirements as to time and form.
32 CFR Section 1803.32: Receipt, recording, and tasking.
32 CFR Section 1803.33: Determination by NACIC Office Chiefs.
32 CFR Section 1803.34: Appeal authority.
32 CFR Section 1803.35: Action by appeals authority.
32 CFR Section 1803.36: Notification of decision and right of further appeal.

SUBPART E—Further Appeals
32 CFR Section 1803.41: Right of further appeal.

32 CFR PART 1804—ACCESS BY HISTORICAL RESEARCHERS AND FORMER PRESIDENTIAL APPOINTEES PURSUANT TO SECTION 4.5 OF EXECUTIVE ORDER 12958

SUBPART A—General
32 CFR Section 1804.1: Authority and purpose.
32 CFR Section 1804.2: Definitions.
32 CFR Section 1804.3: Contact for general information and requests.
32 CFR Section 1804.4: Suggestions and complaints.
32 CFR Section 1804.11: Requirements as to who may apply. 986
32 CFR Section 1804.12: Designations of authority to hear requests. 986
32 CFR Section 1804.13: Receipt, recording, and tasking. 986
32 CFR Section 1804.14: Determinations by tasked officials. 987
32 CFR Section 1804.15: Action by hearing authority. 988
32 CFR Section 1804.16: Action by appeal authority. 988
32 CFR Section 1804.17: Notification of decision. 988
32 CFR Section 1804.18: Termination of access. 988

32 CFR PART 1805—PRODUCTION OF OFFICIAL RECORDS OR DISCLOSURE OF
OFFICIAL INFORMATION IN PROCEEDINGS BEFORE FEDERAL, STATE OR LOCAL
GOVERNMENT ENTITIES OF COMPETENT JURISDICTION 989
32 CFR Section 1805.1: Scope and purpose. 990
32 CFR Section 1805.2: Definitions. 990
32 CFR Section 1805.3: General. 991
32 CFR Section 1805.4: Procedure for production. 991

32 CFR PART 1806—PROCEDURES GOVERNING ACCEPTANCE OF SERVICE OF
PROCESS 993
32 CFR Section 1806.1: Scope and purpose. 993
32 CFR Section 1806.2: Definitions. 993
32 CFR Section 1806.3: Procedures governing acceptance of service of process. 994
32 CFR Section 1806.4: Notification to NACIC Counsel. 995
32 CFR Section 1806.5: Authority of NACIC Counsel. 995

32 CFR PART 1807—ENFORCEMENT OF NONDISCRIMINATION ON THE BASIS OF
DISABILITY IN PROGRAMS OR ACTIVITIES CONDUCTED BY THE NATIONAL
COUNTERINTELLIGENCE CENTER 996
32 CFR Section 1807.101: Purpose. 996
32 CFR Section 1807.102: Application. 996
32 CFR Section 1807.103: Definitions. 997
32 CFR Section 1807.104-1807.110: [Reserved] 999
32 CFR Section 1807.111: Notice. 999
32 CFR Section 1807.112-1807.129: [Reserved] 999
32 CFR Section 1807.130: General prohibitions against discrimination. 999
32 CFR Section 1807.131-1807.139: [Reserved] 1001
32 CFR Section 1807.140: Employment. 1001
32 CFR Section 1807.141-1807.148: [Reserved] 1001
32 CFR Section 1807.149: Program accessibility: discrimination prohibited. 1001
32 CFR Section 1807.150: Program accessibility: existing facilities. 1001
32 CFR Section 1807.151: Program accessibility: new construction and alterations. 1001
32 CFR Section 1807.152-1807.159: [Reserved] 1002
32 CFR Section 1807.160: Communications. 1002
32 CFR Section 1807.161-1807.169: [Reserved] 1003
32 CFR Section 1807.170: Compliance procedures. 1003

32 CFR CHAPTER XIX—CENTRAL INTELLIGENCE AGENCY 1005
32 CFR PART 1900—PUBLIC ACCESS TO CIA RECORDS UNDER THE FREEDOM OF
INFORMATION ACT (FOIA) 1006
32 CFR Section 1900.01: Authority and purpose. 1007
32 CFR Section 1900.02: Definitions. 1007
32 CFR Section 1900.03: Contact for general information and requests. 1010
32 CFR Section 1900.04: Suggestions and complaints. 1010
Filing of FOIA Requests 1011
32 CFR Section 1900.11: Preliminary Information. 1011
32 CFR Section 1900.12: Requirements as to form and content. 1011
32 CFR Section 1900.13: Fees for record services. 1011
32 CFR Section 1900.14: Fee estimates (pre-request option). 1016
CIA Action on FOIA Requests

32 CFR Section 1900.21: Processing of requests for records.

32 CFR Section 1900.22: Action and determination(s) by originator(s) or any interested party.

32 CFR Section 1900.23: Payment of fees, notification of decision, and right of appeal.

Additional Administrative Matters

32 CFR Section 1900.31: Procedures for business information.

32 CFR Section 1900.32: Procedures for information concerning other persons.

32 CFR Section 1900.33: Allocation of resources; agreed extensions of time.

32 CFR Section 1900.34: Requests for expedited processing.

CIA Action on FOIA Administrative Appeals

32 CFR Section 1900.41: Establishment of appeals structure.

32 CFR Section 1900.42: Right of appeal and appeal procedures.

32 CFR Section 1900.43: Determination(s) by Deputy Director(s).

32 CFR Section 1900.44: Action by appeals authority.

32 CFR Section 1900.45: Notification of decision and right of judicial review.

32 CFR PART 1901—PUBLIC RIGHTS UNDER THE PRIVACY ACT OF 1974

General

32 CFR Section 1901.01: Authority and purpose.

32 CFR Section 1901.02: Definitions.

32 CFR Section 1901.03: Contact for general information and requests.

32 CFR Section 1901.04: Suggestions and complaints.

Filing of Privacy Act Requests

32 CFR Section 1901.11: Preliminary information.

32 CFR Section 1901.12: Requirements as to form.

32 CFR Section 1901.13: Requirements as to identification of requester.

32 CFR Section 1901.14: Fees.

Action on Privacy Act Requests

32 CFR Section 1901.21: Processing requests for access to or amendment of records.

32 CFR Section 1901.22: Action and determination(s) by originator(s) or any interested party.

32 CFR Section 1901.23: Notification of decision and right of appeal.

Additional Administrative Matters

32 CFR Section 1901.31: Special procedures for medical and psychological records.

32 CFR Section 1901.32: Requests for expedited processing.

32 CFR Section 1901.33: Allocation of resources; agreed extensions of time.

Action on Privacy Act Administrative Appeals

32 CFR Section 1901.41: Establishment of appeals structure.

32 CFR Section 1901.42: Right of appeal and appeal procedures.

32 CFR Section 1901.43: Determination(s) by Deputy Director(s).

32 CFR Section 1901.44: Action by appeals authority.

32 CFR Section 1901.45: Notification of decision and right of judicial review.

Prohibitions

32 CFR Section 1901.51: Limitations on disclosure.

32 CFR Section 1901.52: Criminal penalties.

Exemptions

32 CFR Section 1901.61: Purpose and authority.

32 CFR Section 1901.62: General exemptions.

32 CFR Section 1901.63: Specific exemptions.

32 CFR PART 1902—INFORMATION SECURITY REGULATIONS

32 CFR Section 1902.13: Declassification and downgrading policy.

32 CFR PART 1903—CONDUCT ON AGENCY INSTALLATIONS
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1903.1</td>
<td>Definitions.</td>
<td>1049</td>
</tr>
<tr>
<td>1903.2</td>
<td>Applicability.</td>
<td>1051</td>
</tr>
<tr>
<td>1903.3</td>
<td>State law applicable.</td>
<td>1051</td>
</tr>
<tr>
<td>1903.4</td>
<td>Vehicles and traffic safety.</td>
<td>1051</td>
</tr>
<tr>
<td>1903.5</td>
<td>Enforcement of parking regulations.</td>
<td>1052</td>
</tr>
<tr>
<td>1903.6</td>
<td>Admission on to an Agency installation.</td>
<td>1053</td>
</tr>
<tr>
<td>1903.7</td>
<td>Trespassing.</td>
<td>1053</td>
</tr>
<tr>
<td>1903.8</td>
<td>Interfering with Agency functions.</td>
<td>1054</td>
</tr>
<tr>
<td>1903.9</td>
<td>Explosives.</td>
<td>1054</td>
</tr>
<tr>
<td>1903.10</td>
<td>Weapons.</td>
<td>1055</td>
</tr>
<tr>
<td>1903.11</td>
<td>Restrictions on photographic, transmitting, and recording equipment.</td>
<td>1055</td>
</tr>
<tr>
<td>1903.12</td>
<td>Alcoholic beverages and controlled substance.</td>
<td>1055</td>
</tr>
<tr>
<td>1903.13</td>
<td>Intoxicated on an Agency installation.</td>
<td>1056</td>
</tr>
<tr>
<td>1903.14</td>
<td>Disorderly conduct.</td>
<td>1056</td>
</tr>
<tr>
<td>1903.15</td>
<td>Preservation of property.</td>
<td>1056</td>
</tr>
<tr>
<td>1903.16</td>
<td>Restriction on animals.</td>
<td>1057</td>
</tr>
<tr>
<td>1903.17</td>
<td>Soliciting, vending, and debt collection.</td>
<td>1057</td>
</tr>
<tr>
<td>1903.18</td>
<td>Distribution of materials.</td>
<td>1057</td>
</tr>
<tr>
<td>1903.19</td>
<td>Gambling.</td>
<td>1057</td>
</tr>
<tr>
<td>1903.20</td>
<td>Penalties and effects on other laws.</td>
<td>1058</td>
</tr>
<tr>
<td>1904.1</td>
<td>Scope and purpose.</td>
<td>1059</td>
</tr>
<tr>
<td>1904.2</td>
<td>Definitions.</td>
<td>1059</td>
</tr>
<tr>
<td>1904.3</td>
<td>Procedures governing acceptance of service of process.</td>
<td>1060</td>
</tr>
<tr>
<td>1904.4</td>
<td>Notification to CIA Office of General Counsel.</td>
<td>1061</td>
</tr>
<tr>
<td>1904.5</td>
<td>Authority of General Counsel.</td>
<td>1061</td>
</tr>
<tr>
<td>1905.1</td>
<td>Scope and purpose.</td>
<td>1062</td>
</tr>
<tr>
<td>1905.2</td>
<td>Definitions.</td>
<td>1062</td>
</tr>
<tr>
<td>1905.3</td>
<td>General.</td>
<td>1063</td>
</tr>
<tr>
<td>1905.4</td>
<td>Procedure for production.</td>
<td>1063</td>
</tr>
<tr>
<td>1906.101</td>
<td>Purpose.</td>
<td>1066</td>
</tr>
<tr>
<td>1906.102</td>
<td>Application.</td>
<td>1067</td>
</tr>
<tr>
<td>1906.103</td>
<td>Definitions.</td>
<td>1067</td>
</tr>
<tr>
<td>1906.104</td>
<td>- 1906.109: [Reserved]</td>
<td>1069</td>
</tr>
<tr>
<td>1906.110</td>
<td>Self-evaluation.</td>
<td>1069</td>
</tr>
<tr>
<td>1906.111</td>
<td>Notice.</td>
<td>1070</td>
</tr>
<tr>
<td>1906.112</td>
<td>- 1906.129: [Reserved]</td>
<td>1070</td>
</tr>
<tr>
<td>1906.130</td>
<td>General prohibitions against discrimination.</td>
<td>1070</td>
</tr>
<tr>
<td>1906.131</td>
<td>- 1906.139: [Reserved]</td>
<td>1071</td>
</tr>
<tr>
<td>1906.140</td>
<td>Employment.</td>
<td>1071</td>
</tr>
<tr>
<td>1906.141</td>
<td>- 1906.148: [Reserved]</td>
<td>1072</td>
</tr>
<tr>
<td>1906.149</td>
<td>Program accessibility: Discrimination prohibited.</td>
<td>1072</td>
</tr>
<tr>
<td>1906.150</td>
<td>Program accessibility: Existing facilities.</td>
<td>1072</td>
</tr>
<tr>
<td>1906.151</td>
<td>Program accessibility: New construction and alterations.</td>
<td>1073</td>
</tr>
<tr>
<td>1906.152</td>
<td>- 1906.159: [Reserved]</td>
<td>1074</td>
</tr>
<tr>
<td>1906.160</td>
<td>Communications.</td>
<td>1074</td>
</tr>
</tbody>
</table>
32 CFR Section 1906.161 - 1906.169: [Reserved] 1074
32 CFR Section 1906.170: Compliance procedures. 1074
32 CFR PART 1907—CHALLENGES TO CLASSIFICATION OF DOCUMENTS BY AUTHORIZED HOLDERS PURSUANT TO § 1.9 OF EXECUTIVE ORDER 12958 1076
General 1077
32 CFR Section 1907.01: Authority and purpose. 1077
32 CFR Section 1907.02: Definitions. 1077
32 CFR Section 1907.03: Contact for general information and requests. 1078
32 CFR Section 1907.04: Suggestions and complaints. 1078
Filing of Challenges 1080
32 CFR Section 1907.11: Prerequisites. 1080
32 CFR Section 1907.12: Requirements as to form. 1080
32 CFR Section 1907.13: Identification of material at issue. 1080
32 CFR Section 1907.14: Transmission. 1080
Action on Challenges 1081
32 CFR Section 1907.21: Receipt, recording, and tasking. 1081
32 CFR Section 1907.22: Challenges barred by res judicata. 1081
32 CFR Section 1907.23: Response by originator(s) and/or any interested party. 1081
32 CFR Section 1907.24: Designation of authority to hear challenges. 1082
32 CFR Section 1907.25: Action on challenge. 1082
32 CFR Section 1907.26: Notification of decision and prohibition on adverse action. 1082
Right of Appeal 1083
32 CFR Section 1907.31: Right of appeal. 1083
32 CFR PART 1908—PUBLIC REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW OF CLASSIFIED INFORMATION PURSUANT TO § 3.6 OF EXECUTIVE ORDER 12958 1084
General 1084
32 CFR Section 1908.01: Authority and purpose. 1084
32 CFR Section 1908.02: Definitions. 1085
32 CFR Section 1908.03: Contact for general information and requests. 1086
32 CFR Section 1908.04: Suggestions and complaints. 1087
32 CFR Section 1908.11: Preliminary information. 1087
32 CFR Section 1908.12: Requirements as to form. 1087
32 CFR Section 1908.13: Fees. 1087
Agency Action on MDR Requests 1088
32 CFR Section 1908.21: Receipt, recording, and tasking. 1088
32 CFR Section 1908.22: Requests barred by res judicata. 1088
32 CFR Section 1908.23: Determination by originator or interested party. 1088
32 CFR Section 1908.24: Notification of decision and right of appeal. 1088
Agency Action on MDR Appeals 1089
32 CFR Section 1908.31: Requirements as to time and form. 1089
32 CFR Section 1908.32: Receipt, recording, and tasking. 1089
32 CFR Section 1908.33: Determination by Deputy Director(s). 1089
32 CFR Section 1908.34: Establishment of appeals structure. 1089
32 CFR Section 1908.35: Action by appeals authority. 1090
32 CFR Section 1908.36: Notification of decision and right of further appeal. 1091
Further Appeals 1091
32 CFR Section 1908.41: Right of further appeal. 1091
32 CFR PART 1909—ACCESS BY HISTORICAL RESEARCHERS AND FORMER PRESIDENTIAL APPOINTEES PURSUANT TO § 4.5 OF EXECUTIVE ORDER 12958 1092
General 1093
32 CFR Section 1909.01: Authority and purpose. 1093
32 CFR Section 1909.02: Definitions. 1093
32 CFR Section 2001.30: Automatic declassification. 1134
32 CFR Section 2001.31: Systematic declassification review. 1139
32 CFR Section 2001.32: Declassification guides. 1139
32 CFR Section 2001.33: Mandatory review for declassification. 1140
32 CFR Section 2001.34: Referrals. 1143
32 CFR Section 2001.35: Discretionary declassification. 1146
32 CFR Section 2001.36: Classified information in the custody of private organizations or individuals. 1146
32 CFR Section 2001.37: Assistance to the Department of State. 1146
SUBPART E—Safeguarding 1148
32 CFR Section 2001.40: General. 1148
32 CFR Section 2001.41: Responsibilities of holders. 1148
32 CFR Section 2001.42: Standards for security equipment. 1149
32 CFR Section 2001.43: Storage. 1149
32 CFR Section 2001.44: Reciprocity of use and inspection of facilities. 1151
32 CFR Section 2001.45: Information controls. 1152
32 CFR Section 2001.46: Transmission. 1153
32 CFR Section 2001.47: Destruction. 1156
32 CFR Section 2001.48: Loss, possible compromise or unauthorized disclosure. 1156
32 CFR Section 2001.49: Special access programs.  
32 CFR Section 2001.50: Telecommunications automated information systems and network security.  
32 CFR Section 2001.53: Open storage areas.  
SUBPART F—Self-Inspections  
SUBPART G—Security Education and Training  
SUBPART H—Standard Forms  
SUBPART I—Reporting and Definitions  
32 CFR Section 2001.91: Other agency reporting requirements.  

32 CFR PART 2003 [RESERVED]  
32 CFR PART 2004—NATIONAL INDUSTRIAL SECURITY PROGRAM DIRECTIVE NO. 1  
SUBPART A—Implementation and Oversight  
32 CFR Section 2004.5: Definitions.  
32 CFR Section 2004.10: Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].  
32 CFR Section 2004.11: Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].  
32 CFR Section 2004.12: Reviews by ISOO [102(b)(4)].  
SUBPART B—Operations  
32 CFR Section 2004.21: Protection of Classified Information [201(e)].  
32 CFR Section 2004.22: Operational Responsibilities [202(a)].  
32 CFR Section 2004.23: Cost Reports [203(d)].  

32 CFR CHAPTER XXI—NATIONAL SECURITY COUNCIL  
32 CFR PART 2102—RULES AND REGULATIONS TO IMPLEMENT THE PRIVACY ACT OF 1974  
32 CFR Section 2102.1: Introduction.  
32 CFR Section 2102.2: Purpose and scope.  
32 CFR Section 2102.3: Definitions.  
32 CFR Section 2102.4: Procedures for determining if an individual is the subject of a record.  
32 CFR Section 2102.13: Requirements for access to a record.  
32 CFR Section 2102.15: Requirements for requests to amend records.  
32 CFR Section 2102.21: Procedures for appeal of determination to deny access to or amendment of requested records.  
32 CFR Section 2102.31: Disclosure of a record to persons other than the individual to whom it pertains.  
32 CFR Section 2102.41: Fees.  
32 CFR Section 2102.51: Penalties.  
32 CFR Section 2102.61: Exemptions.  
32 CFR PART 2103—REGULATIONS TO IMPLEMENT E.O. 12065—INCLUDING PROCEDURES FOR PUBLIC ACCESS TO DOCUMENTS THAT MAY BE DECLASSIFIED.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 CFR Section 2103.1: References.</td>
<td>1192</td>
</tr>
<tr>
<td>32 CFR Section 2103.2: Purpose.</td>
<td>1192</td>
</tr>
<tr>
<td>32 CFR Section 2103.3: Applicability.</td>
<td>1193</td>
</tr>
<tr>
<td>SUBPART B—Original Classification</td>
<td>1193</td>
</tr>
<tr>
<td>32 CFR Section 2103.11: Basic policy.</td>
<td>1193</td>
</tr>
<tr>
<td>32 CFR Section 2103.12: Level of original classification.</td>
<td>1193</td>
</tr>
<tr>
<td>32 CFR Section 2103.13: Duration of original classification.</td>
<td>1193</td>
</tr>
<tr>
<td>32 CFR Section 2103.14: Challenges to classification.</td>
<td>1193</td>
</tr>
<tr>
<td>SUBPART C—Derivative Classification</td>
<td>1195</td>
</tr>
<tr>
<td>32 CFR Section 2103.21: Definition and application.</td>
<td>1195</td>
</tr>
<tr>
<td>SUBPART D—Declassification and Downgrading</td>
<td>1196</td>
</tr>
<tr>
<td>32 CFR Section 2103.31: Declassification authority.</td>
<td>1196</td>
</tr>
<tr>
<td>32 CFR Section 2103.32: Mandatory review for declassification.</td>
<td>1196</td>
</tr>
<tr>
<td>32 CFR Section 2103.33: Downgrading authority.</td>
<td>1197</td>
</tr>
<tr>
<td>SUBPART E—Safeguarding</td>
<td>1198</td>
</tr>
<tr>
<td>32 CFR Section 2103.41: Reproduction controls.</td>
<td>1198</td>
</tr>
<tr>
<td>SUBPART F—Implementation and Review</td>
<td>1199</td>
</tr>
<tr>
<td>32 CFR Section 2103.51: Information Security Oversight Committee.</td>
<td>1199</td>
</tr>
<tr>
<td>32 CFR Section 2103.52: Classification Review Committee.</td>
<td>1199</td>
</tr>
<tr>
<td>32 CFR PART 2400—REGULATIONS TO IMPLEMENT E.O. 12356; OFFICE OF SCIENCE AND TECHNOLOGY POLICY INFORMATION SECURITY PROGRAM</td>
<td>1200</td>
</tr>
<tr>
<td>SUBPART A—General Provisions</td>
<td>1202</td>
</tr>
<tr>
<td>32 CFR Section 2400.1: Authority.</td>
<td>1202</td>
</tr>
<tr>
<td>32 CFR Section 2400.2: Purpose.</td>
<td>1202</td>
</tr>
<tr>
<td>32 CFR Section 2400.3: Applicability.</td>
<td>1202</td>
</tr>
<tr>
<td>32 CFR Section 2400.4: Atomic Energy Material.</td>
<td>1202</td>
</tr>
<tr>
<td>SUBPART B—Original Classification</td>
<td>1203</td>
</tr>
<tr>
<td>32 CFR Section 2400.5: Basic policy.</td>
<td>1203</td>
</tr>
<tr>
<td>32 CFR Section 2400.6: Classification levels.</td>
<td>1203</td>
</tr>
<tr>
<td>32 CFR Section 2400.7: Original classification authority.</td>
<td>1203</td>
</tr>
<tr>
<td>32 CFR Section 2400.8: Limitations on delegation of original classification authority.</td>
<td>1204</td>
</tr>
<tr>
<td>32 CFR Section 2400.9: Classification requirements.</td>
<td>1204</td>
</tr>
<tr>
<td>32 CFR Section 2400.10: Presumption of damage.</td>
<td>1205</td>
</tr>
<tr>
<td>32 CFR Section 2400.11: Duration of classification.</td>
<td>1205</td>
</tr>
<tr>
<td>32 CFR Section 2400.12: Identification and markings.</td>
<td>1206</td>
</tr>
<tr>
<td>32 CFR Section 2400.13: Limitations on classification.</td>
<td>1207</td>
</tr>
<tr>
<td>SUBPART C—Derivative Classification</td>
<td>1208</td>
</tr>
<tr>
<td>32 CFR Section 2400.14: Use of derivative classification.</td>
<td>1208</td>
</tr>
<tr>
<td>32 CFR Section 2400.15: Classification guides.</td>
<td>1208</td>
</tr>
<tr>
<td>32 CFR Section 2400.16: Derivative classification markings.</td>
<td>1209</td>
</tr>
<tr>
<td>SUBPART D—Declassification and Downgrading</td>
<td>1210</td>
</tr>
<tr>
<td>32 CFR Section 2400.17: Policy.</td>
<td>1210</td>
</tr>
<tr>
<td>32 CFR Section 2400.18: Declassification and downgrading authority.</td>
<td>1210</td>
</tr>
<tr>
<td>32 CFR Section 2400.19: Declassification by the Director of the Information Security Oversight Office.</td>
<td>1210</td>
</tr>
<tr>
<td>32 CFR Section 2400.20: Systematic review for declassification.</td>
<td>1210</td>
</tr>
<tr>
<td>32 CFR Section 2400.21: Mandatory review for declassification.</td>
<td>1211</td>
</tr>
<tr>
<td>32 CFR Section 2400.22: Freedom of Information Act and Privacy Act requests.</td>
<td>1213</td>
</tr>
<tr>
<td>32 CFR Section 2400.23: Prohibition.</td>
<td>1214</td>
</tr>
<tr>
<td>32 CFR Section 2400.24: Downgrading.</td>
<td>1214</td>
</tr>
<tr>
<td>SUBPART E—Safeguarding</td>
<td>1215</td>
</tr>
<tr>
<td>32 CFR Section 2400.25: Access.</td>
<td>1215</td>
</tr>
</tbody>
</table>
32 CFR PART 2800—SECURITY PROCEDURES ........................................ 1235
32 CFR Section 2800.1: Purpose ....................................................... 1236
32 CFR Section 2800.2: Guiding directives ........................................ 1236
32 CFR Section 2800.3: Policy ......................................................... 1236
32 CFR Section 2800.4: General information ...................................... 1236
32 CFR Section 2800.5: Policies ....................................................... 1242
32 CFR Section 2800.6: Delegation of classification and declassification authority. ....................................................... 1243
32 CFR Section 2800.7: Designation of chairperson for Ad Hoc Committees. ....................................................... 1243

NON-LEGISLATIVE AND OTHER AGENCY RULES ............................ 1244

Department of Defense Regulation 5240.1-R: Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons ........................................................................................................ 1245

REFERENCES ..................................................................................... 1248

DL1. DEFINITIONS .............................................................................. 1249
DL1.1. Administrative Purposes ............................................................ 1249
DL1.1.2. Available Publicly ................................................................. 1249
DL1.1.3. Communications Security .................................................... 1249
DL1.1.4. Consent .............................................................................. 1249
DL1.1.5. Counterintelligence ............................................................... 1249
DL1.1.6. Counterintelligence Investigation ......................................... 1250
DL1.1.7. DoD Component .................................................................. 1250
DL1.1.8. DoD Intelligence Components ............................................. 1250
DL1.1.9. Electronic Surveillance ......................................................... 1250
DL1.1.10. Employee ........................................................................ 1251
DL1.1.11. Foreign Intelligence ............................................................ 1251
DL1.1.12. Foreign Power .................................................................. 1251
DL1.1.13. Intelligence Activities .......................................................... 1251
DL1.1.14. Intelligence Community and an Agency of Or Within the Intelligence Community .......................................................... 1251
DL1.1.15. International Narcotics Activities ......................................... 1251
DL1.1.16. International Terrorist Activities ......................................... 1252
DL1.1.17. Lawful Investigation ............................................................. 1252
DL1.1.18. Personnel Security ............................................................... 1252
DL1.1.20. Physical Security ................................................................. 1253
DL1.1.22. Reasonable Belief ............................................................... 1253
DL1.1.23. Signals Intelligence ............................................................. 1253
DL1.1.24. United States ................................................................... 1253
DL1.1.25. United States Person .......................................................... 1253

C1. CHAPTER 1: PROCEDURE 1. GENERAL PROVISIONS ................. 1255
C1.1. APPLICABILITY AND SCOPE .................................................. 1255
C1.2. PURPOSE ................................................................................ 1255
C1.3. INTERPRETATION ................................................................... 1255
C1.4. EXCEPTIONS TO POLICY ....................................................... 1256
C1.5. AMENDMENT ........................................................................ 1256

C2. CHAPTER 2: PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS ........................................ 1257
C2.1. APPLICABILITY AND SCOPE .................................................. 1257
C2.2. EXPLANATION OF UNDEFINED TERMS ................................. 1257
C2.2.1. When Information is Considered to be “Collected” ..................... 1257
C2.2.2. “Cooperating Sources” ......................................................... 1257

Page 48
Department of Defense Directive 5240.01

SUBJECT: DoD Intelligence Activities

References:

1. REISSUANCE AND PURPOSE
2. APPLICABILITY AND SCOPE
3. DEFINITIONS
4. POLICY
5. RESPONSIBILITIES
6. EFFECTIVE DATE

Enclosures – 2

E1. ENCLOSURE 1 - REFERENCES, continued
E2. ENCLOSURE 2 - DEFINITIONS

The Attorney General’s Guidelines for Domestic FBI Operations

PREAMBLE

INTRODUCTION

A. FBI RESPONSIBILITIES—FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE

1. Federal Crimes
2. Threats to the National Security
3. Foreign Intelligence

B. THE FBI AS AN INTELLIGENCE AGENCY

C. OVERSIGHT

I. GENERAL AUTHORITIES AND PRINCIPLES

A. SCOPE
B. GENERAL AUTHORITIES
C. USE OF AUTHORITIES AND METHODS

1. Protection of the United States and Its People
2. Choice of Methods
3. Respect for Legal Rights
4. Undisclosed Participation in Organizations
5. Maintenance of Records under the Privacy Act

D. NATURE AND APPLICATION OF THE GUIDELINES

1. Repealers
2. Status as Internal Guidance
3. Departures from the Guidelines
4. Other Activities Not Limited

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

A. ASSESSMENTS
1. Purposes
2. Approval
3. Authorized Activities
4. Authorized Methods

B. PREDICATED INVESTIGATIONS
1. Purposes
2. Approval
3. Circumstances Warranting Investigation
4. Preliminary and Full Investigations
5. Notice Requirements
C. ENTERPRISE INVESTIGATIONS
   1. Definition
   2. Scope
   3. Notice and Reporting Requirements
III. ASSISTANCE TO OTHER AGENCIES
   A. THE INTELLIGENCE COMMUNITY
   B. FEDERAL AGENCIES GENERALLY
      1. In General
      2. The President in Relation to Civil Disorders
      3. Public Health and Safety Authorities in Relation to Demonstrations
   C. STATE, LOCAL, OR TRIBAL AGENCIES
   D. FOREIGN AGENCIES
   E. APPLICABLE STANDARDS AND PROCEDURES
IV. INTELLIGENCE ANALYSIS AND PLANNING
   A. STRATEGIC INTELLIGENCE ANALYSIS
   B. REPORTS AND ASSESSMENTS GENERALLY
   C. INTELLIGENCE SYSTEMS
V. AUTHORIZED METHODS
   A. PARTICULAR METHODS
   B. SPECIAL REQUIREMENTS
      1. Contacts with Represented Persons
      2. Use of Classified Investigative Technologies
   C. OTHERWISE ILLEGAL ACTIVITY
VI. RETENTION AND SHARING OF INFORMATION
   A. RETENTION OF INFORMATION
   B. INFORMATION SHARING GENERALLY
      1. Permissive Sharing
      2. Required Sharing
   C. INFORMATION RELATING TO CRIMINAL MATTERS
      1. Coordination with Prosecutors
      2. Criminal Matters Outside FBI Jurisdiction
      3. Reporting of Criminal Activity
   D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS
      1. Department of Justice
      2. White House
      3. Special Statutory Requirements
VII. DEFINITIONS
   A. CONSENSUAL MONITORING:
   B. EMPLOYEE:
   C. FOR OR ON BEHALF OF A FOREIGN POWER:
   D. FOREIGN COMPUTER INTRUSION:
   E. FOREIGN INTELLIGENCE:
   F. FOREIGN INTELLIGENCE REQUIREMENTS:
   G. FOREIGN POWER:
   H. HUMAN SOURCE:
   I. INTELLIGENCE ACTIVITIES:
   J. INTERNATIONAL TERRORISM:
   K. PROPRTETARY:
   L. PUBLICLY AVAILABLE:
   M. RECORDS:
JUDICIAL BRANCH RULES 1347

Foreign Intelligence Surveillance Court Rules 1348
I. Scope, Construction, and Amendment of Rules 1348
   Rule 1: Scope of Rules 1348
   Rule 2: Amendment 1348
II. National Security Information 1348
   Rule 3: 1348
III. Structure of the Court and Authority of Judges 1349
   Rule 4: Structure 1349
   Rule 5: Authority of the Judges 1349
IV. Attorneys Authorized to Appear Before the Court 1349
   Rule 6: License and Other Requirements for Attorneys 1349
V. Clerk's Office 1350
   Rule 7: Duties of the Clerk 1350
VI. Form and Filing of Applications for Court Orders 1350
   Rule 8: Form of Applications for Court Order 1350
   Rule 9: Time of Submission; Applications 1351
   Rule 10: New Matters; Supplementation 1351
   Rule 11: Motions 1352
   Rule 12: Applications Following Approval of Emergency Authorizations 1352
VII. Hearings 1352
   Rule 13: Hearings 1352
VIII. Orders 1353
   Rule 14: Contents 1353
   Rule 15: Enforcement; Sanctions 1353
   Rule 16: Returns; Time for Filing; Contents 1354
IX. Sequestration or Destruction 1354
   Rule 17: Sequestration or Destruction 1354
X. Appeals 1354
   Rule 18: Motion to Transmit Record 1354
   Rule 19: Transmission of the Record 1355
   Rule 20: Oral Notification to the Court of Review 1355
Appendix to the FISA Court Rules: Procedures for Review of Petitions Filed Pursuant to Section 501(F) of the Foreign Intelligence Surveillance Court Act of 1978 1356
I: IN GENERAL 1356
   § 1: Limited Scope 1356
   § 2: Rules of the Foreign Intelligence Surveillance Court Apply 1356
II: PETITION AND OTHER PAPERS 1357
   § 3: Filing 1357
   § 4: Content of Petition 1358
   § 5: Form and Length of Petition and Other Papers 1358
   § 6: Service 1359
   § 7: Computation of Time 1359
   § 8: Notifying Presiding Judge 1359
III: ASSIGNMENT TO A JUDGE 1360
PRESIDENTIAL RULES
Executive Orders Relevant to U.S. Intelligence Law
Executive Order 10865. Safeguarding Classified Information Within Industry


WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosures of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that those provisions and procedures recognize the interest of individuals affected thereby and provide maximum possible safeguards to protect such interests:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the armed forces of the United States, it is hereby ordered as follows:

Section 1. When used in this order, the term “head of a department” means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Secretary of Homeland Security, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term “head of a department” also means the head of any department or agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829 [set out below].

Sec. 2. An authorization for access to classified information pursuant to Executive Order No. 12829 [set out below] may be granted by the head of a department or his designee, including but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an “applicant”, for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.
Sec. 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked pursuant to Executive Order No. 12829 [set out below] by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of the reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the department concerned, an opportunity to appear personally before the head of the department concerned or his designee including, but not limited to, those officials named in section 8 of this order for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

Sec. 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.
(2) The head of the department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the department to be good and sufficient.

(b) Whenever procedures under paragraphs (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

Sec. 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the department concerned by an investigative agency pursuant to its responsibilities in connection with assisting the head of the department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered. In such instances a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.
Sec. 6. The head of a department of the United States or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, and the proceeding involves the activity in connection with which the witness is employed, travel expenses and per diem are authorized as provided by the Standardized Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees of the executive branch of the Government or members of the armed forces of the United States not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An officer or employee of the executive branch of the Government or a member of the armed forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other department or agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination.

Sec. 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

Sec. 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a department by this order may be delegated to the the [sic] deputy of that department, or the principal assistant to the head of that department, as the case may be.

Sec. 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

Modification of Executive Order No. 10865
Executive Order 12139. Exercise of Certain Authority Respecting Electronic Surveillance


By the authority vested in me as President by Sections 102 and 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802 and 1804), in order to provide as set forth in that Act [this chapter] for the authorization of electronic surveillance for foreign intelligence purposes, it is hereby ordered as follows:

1–101. Pursuant to Section 102(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802(a)), the Attorney General is authorized to approve electronic surveillance to acquire foreign intelligence information without a court order, but only if the Attorney General makes the certifications required by that Section.

1–102. Pursuant to Section 102(b) of the Foreign Intelligence Act of 1978 (50 U.S.C. 1802(b)), the Attorney General is authorized to approve applications to the court having jurisdiction under Section 103 of that Act [50 U.S.C. 1803] to obtain orders for electronic surveillance for the purpose of obtaining foreign intelligence information.

1–103. Pursuant to Section 104(a)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804(a)(6)), the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by Section 104(a)(6) of the Act in support of applications to conduct electronic surveillance:

(a) Secretary of State.

(b) Secretary of Defense.

(c) Director of National Intelligence.

(d) Director of the Federal Bureau of Investigation.

(e) Deputy Secretary of State.

(f) Deputy Secretary of Defense.

(g) Director of the Central Intelligence Agency.

(h) Principal Deputy Director of National Intelligence.
(i) Deputy Director of the Federal Bureau of Investigation.

None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President with the advice and consent of the Senate. The requirement of the preceding sentence that the named official must be appointed by the President with the advice and consent of the Senate does not apply to the Deputy Director of the Federal Bureau of Investigation.

1–104. Section 2–202 of Executive Order No. 12036 [set out under section 401 of this title] is amended by inserting the following at the end of that section: “Any electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act as well as this Order.”.

1–105. Section 2–203 of Executive Order No. 12036 [set out under section 401 of this title] is amended by inserting the following at the end of that section: “Any monitoring which constitutes electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978 shall be conducted in accordance with that Act as well as this Order.”.
Executive Order 12333. United States Intelligence Activities


TABLE OF CONTENTS

➤ PART 1—GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS
  o 1.1 Goals
  o 1.2 The National Security Council
  o 1.3 Director of National Intelligence
  o 1.4 The Intelligence Community
  o 1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies
  o 1.6 Heads of Elements of the Intelligence Community
  o 1.7 Intelligence Community Elements
  o 1.8 The Department of State
  o 1.9 The Department of the Treasury
  o 1.10 The Department of Defense
  o 1.11 The Department of Homeland Security
  o 1.12 The Department of Energy
  o 1.13 The Federal Bureau of Investigation

➤ PART 2—CONDUCT OF INTELLIGENCE ACTIVITIES
  o 2.1 Need
  o 2.2 Purpose
  o 2.3 Collection of Information
  o 2.4 Collection Techniques
  o 2.5 Attorney General Approval
  o 2.6 Assistance to Law Enforcement and other Civil Authorities
  o 2.7 Contracting
  o 2.8 Consistency With Other Laws
  o 2.9 Undisclosed Participation in Organizations Within the United States
  o 2.10 Human Experimentation
  o 2.11 Prohibition on Assassination
  o 2.12 Indirect Participation
  o 2.13 Limitation on Covert Action

➤ PART 3—GENERAL PROVISIONS
  o 3.1 Congressional Oversight
  o 3.2 Implementation
  o 3.3 Procedures
Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended (Act) [see Short Title note above], and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1—GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS

1.1 Goals

The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:
(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

(2) Threats to the United States and its interests from terrorism; and

(3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 The National Security Council

(a) Purpose. The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) Covert Action and Other Sensitive Intelligence Operations. The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.
1.3 Director of National Intelligence

Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108–458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;

(2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;
(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:
(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.
(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;
(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and
(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director’s exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director’s authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director’s intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.
(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head’s intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

### 1.4 The Intelligence Community

Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;
(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments’ and, as appropriate, private sector entities’ information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies

The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;
(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;

(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the
Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

**1.6 Heads of Elements of the Intelligence Community**

The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective
organizations have access to any information or intelligence necessary to perform their official duties.

1.7 Intelligence Community Elements

Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93–148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.
(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

(3) Conduct counterintelligence activities;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;
(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and
(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and
defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 The Department of State

In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:
(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 The Department of the Treasury

In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 The Department of Defense

The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;

(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;
(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in [sub]sections (a) through [sic] (i) above, and to support the Intelligence Community elements of the Department of Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense, (h) above to carry out the Secretary of Defense’s responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 The Department of Homeland Security

In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.
1.12 The Department of Energy

In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 The Federal Bureau of Investigation

In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2—CONDUCT OF INTELLIGENCE ACTIVITIES

2.1 Need

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 Purpose

This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance

Page 85
between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 Collection of Information

Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques

Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element concerned and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of
probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a nonintelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 Assistance to Law Enforcement and other Civil Authorities

Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element within the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting

Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws

Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States

No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person’s intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.
2.10 Human Experimentation

No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 Prohibition on Assassination

No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination.

2.12 Indirect Participation

No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 Limitation on Covert Action

No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3—GENERAL PROVISIONS

3.1 Congressional Oversight

The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act [50 U.S.C. 413 et seq.]. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 Implementation

The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable
to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 Procedures

The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 References and Transition

References to “Senior Officials of the Intelligence Community” or “SOICs” in executive orders or other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 Definitions

For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community and elements of the Intelligence Community* refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;
(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) National Intelligence and Intelligence Related to National Security means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) The National Intelligence Program means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.
(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

### 3.6 Revocation

Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

### 3.7 General Provisions

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

[For provisions relating to consideration of Commandant and Assistant Commandant for Intelligence of the Coast Guard as a “Senior Official of the Intelligence Community” for purposes of Ex. Ord. No. 12333, set out above, and all other relevant authorities, see Ex. Ord. No. 13286, §87, Feb. 28, 2003, 68 F.R. 10632, set out as a note under section 111 of Title 6, Domestic Security.]
Executive Order 12829. National Industrial Security Program


This order establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses, and grants to nongovernment organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of Government. The national security also requires that our industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the National Industrial Security Program shall serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation’s economic and technological interests.

Therefore, by the authority vested in me as President by the Constitution and the laws of the United States of America, including the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011–2286) [42 U.S.C. 2011 et seq.], the National Security Act of 1947, as amended (codified as amended in scattered sections of the United States Code) [see Short Title note set out under section 401 of this title], and the Federal Advisory Committee Act, as amended (5 U.S.C. App. 2) [5 U.S.C. App.], it is hereby ordered as follows:

PART 1. ESTABLISHMENT AND POLICY

Section 101. Establishment.

(a) There is established a National Industrial Security Program. The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. For the purposes of this order, the terms “contractor, licensee, or grantee” means current, prospective, or former contractors, licensees, or grantees of United States agencies. The National Industrial Security Program shall be applicable to all executive branch departments and agencies.

(b) The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order No. 12356 of April 2, 1982 [formerly set out above], or its successor, and the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 et seq.].
(c) For the purposes of this order, the term “contractor” does not include individuals engaged under personal services contracts.

Sec. 102. Policy Direction.

(a) The National Security Council shall provide overall policy direction for the National Industrial Security Program.

(b) The Director of the Information Security Oversight Office, established under Executive Order No. 12356 of April 2, 1982 [formerly set out above], shall be responsible for implementing and monitoring the National Industrial Security Program and shall:

(1) develop, in consultation with the agencies, and promulgate subject to the approval of the National Security Council, directives for the implementation of this order, which shall be binding on the agencies;

(2) oversee agency, contractor, licensee, and grantee actions to ensure compliance with this order and implementing directives;

(3) review all agency implementing regulations, internal rules, or guidelines. The Director shall require any regulation, rule, or guideline to be changed if it is not consistent with this order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation, rule, or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority, pursuant to terms of applicable contracts, licenses, grants, or regulations, to conduct on-site reviews of the implementation of the National Industrial Security Program by each agency, contractor, licensee, and grantee that has access to or stores classified information and to require of each agency, contractor, licensee, and grantee those reports, information, and other cooperation that may be necessary to fulfill the Director’s responsibilities. If these reports, inspections, or access to specific classified information, or other forms of cooperation, would pose an exceptional national security risk, the affected agency head or the senior official designated under section 203(a) of this order may request the National Security Council to deny access to the Director. The Director shall not have access pending a prompt decision by the National Security Council;

(5) report any violations of this order or its implementing directives to the head of the agency or to the senior official designated under section 203(a) of this order so that corrective action, if appropriate, may be taken. Any such report pertaining to the implementation of the National Industrial Security Program by a contractor, licensee, or grantee shall be directed to the agency that is exercising
operational oversight over the contractor, licensee, or grantee under section 202 of this order;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the National Industrial Security Program;

(7) consider, in consultation with the advisory committee established by this order, affected agencies, contractors, licensees, and grantees, and recommend to the President through the National Security Council changes to this order; and

(8) report at least annually to the President through the National Security Council on the implementation of the National Industrial Security Program.

(c) Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 et seq.], or the authority of the Director of Central Intelligence under the National Security Act of 1947, as amended [see Short Title note set out under section 401 of this title], or Executive Order No. 12333 of December 8, 1981 [50 U.S.C. 401 note].


(a) Establishment. There is established the National Industrial Security Program Policy Advisory Committee (“Committee”). The Director of the Information Security Oversight Office shall serve as Chairman of the Committee and appoint the members of the Committee. The members of the Committee shall be the representatives of those departments and agencies most affected by the National Industrial Security Program and nongovernment representatives of contractors, licensees, or grantees involved with classified contracts, licenses, or grants, as determined by the Chairman.

(b) Functions. (1) The Committee members shall advise the Chairman of the Committee on all matters concerning the policies of the National Industrial Security Program, including recommended changes to those policies as reflected in this order, its implementing directives, or the operating manual established under this order, and serve as a forum to discuss policy issues in dispute.

(2) The Committee shall meet at the request of the Chairman, but at least twice during the calendar year.

(c) Administration. (1) Members of the Committee shall serve without compensation for their work on the Committee. However, nongovernment members may be allowed travel expenses, including per diem in lieu of

(2) To the extent permitted by law and subject to the availability of funds, the Administrator of General Services shall provide the Committee with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(d) General. Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended [5 U.S.C. App.], except that of reporting to the Congress, which are applicable to the Committee, shall be performed by the Administrator of General Services in accordance with the guidelines and procedures established by the General Services Administration.

**PART 2. OPERATIONS**


(a) The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence, shall issue and maintain a National Industrial Security Program Operating Manual (“Manual”). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 et seq.]. The Director of Central Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information.

(b) The Manual shall prescribe specific requirements, restrictions, and other safeguards that are necessary to preclude unauthorized disclosure and control authorized disclosure of classified information to contractors, licensees, or grantees. The Manual shall apply to the release of classified information during all phases of the contracting process including bidding, negotiation, award, performance, and termination of contracts, the licensing process, or the grant process, with or under the control of departments or agencies.

(c) The Manual shall also prescribe requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information.
(d) In establishing particular requirements, restrictions, and other safeguards within the Manual, the Secretary of Defense, the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence shall take into account these factors: (i) the damage to the national security that reasonably could be expected to result from an unauthorized disclosure; (ii) the existing or anticipated threat to the disclosure of information; and (iii) the short- and long-term costs of the requirements, restrictions, and other safeguards.

(e) To the extent that is practicable and reasonable, the requirements, restrictions, and safeguards that the Manual establishes for the protection of classified information by contractors, licensees, and grantees shall be consistent with the requirements, restrictions, and safeguards that directives implementing Executive Order No. 12356 of April 2, 1982 [formerly set out above], or the Atomic Energy Act of 1954, as amended, establish for the protection of classified information by agencies. Upon request by the Chairman of the Committee, the Secretary of Defense shall provide an explanation and justification for any requirement, restriction, or safeguard that results in a standard for the protection of classified information by contractors, licensees, and grantees that differs from the standard that applies to agencies.

(f) The Manual shall be issued to correspond as closely as possible to pertinent decisions of the Secretary of Defense and the Director of Central Intelligence made pursuant to the recommendations of the Joint Security Review Commission and to revisions to the security classification system that result from Presidential Review Directive 29, but in any event no later than June 30, 1994.


(a) The Secretary of Defense shall serve as Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, and grantees and their respective employees. The heads of agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads.

(b) The Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf.

(c) The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to information under their respective programs classified
under the Atomic Energy Act of 1954, as amended [42 U.S.C. 2011 et seq.]. The Secretary or the Commission may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on behalf of the Secretary or the Commission, respectively.

(d) The Executive Agent shall have the authority to issue, after consultation with affected agencies, standard forms or other standardization that will promote the implementation of the National Industrial Security Program.

Sec. 203. Implementation.

(a) The head of each agency that enters into classified contracts, licenses, or grants shall designate a senior agency official to direct and administer the agency’s implementation and compliance with the National Industrial Security Program.

(b) Agency implementing regulations, internal rules, or guidelines shall be consistent with this order, its implementing directives, and the Manual. Agencies shall issue these regulations, rules, or guidelines no later than 180 days from the issuance of the Manual. They may incorporate all or portions of the Manual by reference.

(c) Each agency head or the senior official designated under paragraph (a) above shall take appropriate and prompt corrective action whenever a violation of this order, its implementing directives, or the Manual occurs.

(d) The senior agency official designated under paragraph (a) above shall account each year for the costs within the agency associated with the implementation of the National Industrial Security Program. These costs shall be reported to the Director of the Information Security Oversight Office, who shall include them in the reports to the President prescribed by this order.

(e) The Secretary of Defense, with the concurrence of the Administrator of General Services, the Administrator of the National Aeronautics and Space Administration, and such other agency heads or officials who may be responsible, shall amend the Federal Acquisition Regulation to be consistent with the implementation of the National Industrial Security Program.

(f) All contracts, licenses, or grants that involve access to classified information and that are advertised or proposed following the issuance of agency regulations, rules, or guidelines described in paragraph (b) above shall comply with the National Industrial Security Program. To the extent that is feasible, economical, and permitted by law, agencies shall amend, modify, or convert preexisting
contracts, licenses, or grants, or previously advertised or proposed contracts, licenses, or grants, that involve access to classified information for operation under the National Industrial Security Program. Any direct inspection or monitoring of contractors, licensees, or grantees specified by this order shall be carried out pursuant to the terms of a contract, license, grant, or regulation.

(g) Executive Order No. 10865 of February 20, 1960 [set out above], as amended by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, is hereby amended as follows:

(1) Section 1(a) and (b) are revoked as of the effective date of this order.

(2) Section 1(c) is renumbered as Section 1 and is amended to read as follows:

“Section 1. When used in this order, the term ‘head of a department’ means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term ‘head of a department’ also means the head of any department or agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829.”

(3) Section 2 is amended by inserting the words “pursuant to Executive Order No. 12829” after the word “information.”

(4) Section 3 is amended by inserting the words “pursuant to Executive Order No. 12829” between the words “revoked” and “by” in the second clause of that section.

(5) Section 6 is amended by striking out the words “The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Secretary of Transportation, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section (1)(b),” at the beginning of the first sentence, and inserting in their place “The head of a department of the United States . . . .”

(6) Section 8 is amended by striking out paragraphs (1) through (7) and inserting in their place “. . . . the deputy of that department, or the principal assistant to the head of that department, as the case may be.”

(h) All delegations, rules, regulations, orders, directives, agreements, contracts, licenses, and grants issued under preexisting authorities, including section 1(a)
and (b) of Executive Order No. 10865 of February 20, 1960, as amended, by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, shall remain in full force and effect until amended, modified, or terminated pursuant to authority of this order.

(i) This order shall be effective immediately.
Executive Order 12937. Declassification of Selected Records Within National Archives of United States

Ex. Ord. No. 12937, Nov. 10, 1994, 59 F.R. 59097, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. The records in the National Archives of the United States referenced in the list accompanying this order are hereby declassified.

Sec. 2. The Archivist of the United States shall take such actions as are necessary to make such records available for public research no later than 30 days from the date of this Order, except to the extent that the head of an affected agency and the Archivist have determined that specific information within such records must be protected from disclosure pursuant to an authorized exemption to the Freedom of Information Act, 5 U.S.C. 552, other than the exemption that pertains to national security information.

Sec. 3. Nothing contained in this order shall create any right or benefit, substantive or procedural, enforceable by any party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

William J. Clinton.

Records in the following record groups (“RG”) in the National Archives of the United States shall be declassified. Page numbers are approximate. A complete list of the selected records is available from the Archivist of the United States.

I. All unreviewed World War II and earlier records, including:

| A.  | RG 18, Army Air Forces               | 1,722,400 pp. |
| C.  | RG 127, United States Marine Corps   | 195,000 pp. |
| E.  | RG 226, Office of Strategic Services | 415,000 pp. |
| F.  | RG 60, United States Occupation Headquarters | 4,422,500 pp. |
| H.  | RG 332, United States Theaters of War, World War II | 1,182,500 pp. |
I. RG 338, Mediterranean Theater of Operations and European Command

Subtotal for World War II and earlier

II. Post-1945 Collections (Military and Civil)

A. RG 19, Bureau of Ships, Pre-1950 General Correspondence (selected records)

B. RG 51, Bureau of the Budget, 52.12 Budget Preparation Branch, 1952–69

C. RG 72, Bureau of Aeronautics (Navy) (selected records)

D. RG 166, Foreign Agricultural Service, Narrative Reports, 1955–61

E. RG 313, Naval Operating Forces (selected records)

F. RG 319, Office of the Chief of Military History Manuscripts and Background Papers (selected records)

G. RG 337, Headquarters, Army Ground Forces (selected records)

H. RG 341, Headquarters, United States Air Force (selected records)

I. RG 389, Office of the Provost Marshal General (selected records)

J. RG 391, United States Army Regular Army Mobil Units

K. RG 428, General Records of the Department of the Navy (selected records)

L. RG 472, Army Vietnam Collection (selected records)

Subtotal for Other

TOTAL

pp. 9,500,000

21.0 million

1,732,500 pp.

142,500 pp.

5,655,000 pp.

1,272,500 pp.

407,500 pp.

933,000 pp.

1,269,700 pp.

4,870,000 pp.

448,000 pp.

240,000 pp.

31,250 pp.

5,864,000 pp.

22.9 million pp.

43.9 million pp.
Executive Order 12949. Foreign Intelligence Physical Searches


By the authority vested in me as President by the Constitution and the laws of the United States, including sections 302 and 303 of the Foreign Intelligence Surveillance Act of 1978 (“Act”) (50 U.S.C. 1801, et seq.), as amended by Public Law 103–359 [50 U.S.C. 1822, 1823], and in order to provide for the authorization of physical searches for foreign intelligence purposes as set forth in the Act, it is hereby ordered as follows:

Section 1. Pursuant to section 302(a)(1) of the Act, the Attorney General is authorized to approve physical searches, without a court order, to acquire foreign intelligence information for periods of up to one year, if the Attorney General makes the certifications required by that section.

Sec. 2. Pursuant to section 302(b) of the Act, the Attorney General is authorized to approve applications to the Foreign Intelligence Surveillance Court under section 303 of the Act to obtain orders for physical searches for the purpose of collecting foreign intelligence information.

Sec. 3. Pursuant to section 303(a)(6) of the Act, the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by section 303(a)(6) of the Act in support of applications to conduct physical searches:

(a) Secretary of State;

(b) Secretary of Defense;

[(c)] Director of National Intelligence;

(d) Director of the Federal Bureau of Investigation,

(e) Deputy Secretary of State;

(f) Deputy Secretary of Defense;

(g) Director of the Central Intelligence Agency;

(h) Principal Deputy Director of National Intelligence; and
(i) Deputy Director of the Federal Bureau of Investigation.

None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President, by and with the advice and consent of the Senate. The requirement of the preceding sentence that the named official must be appointed by the President with the advice and consent of the Senate does not apply to the Deputy Director of the Federal Bureau of Investigation.
Executive Order 12951. Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems

Ex. Ord. No. 12951, Feb. 22, 1995, 60 F.R. 10789, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to release certain scientifically or environmentally useful imagery acquired by space-based national intelligence reconnaissance systems, consistent with the national security, it is hereby ordered as follows:

Section 1. Public Release of Historical Intelligence Imagery.

Imagery acquired by the space-based national intelligence reconnaissance systems known as the Corona, Argon, and Lanyard missions shall, within 18 months of the date of this order, be declassified and transferred to the National Archives and Records Administration with a copy sent to the United States Geological Survey of the Department of the Interior consistent with procedures approved by the Director of Central Intelligence and the Archivist of the United States. Upon transfer, such imagery shall be deemed declassified and shall be made available to the public.

Section 2. Review for Future Public Release of Intelligence Imagery.

(a) All information that meets the criteria in section 2(b) of this order shall be kept secret in the interests of national defense and foreign policy until deemed otherwise by the Director of Central Intelligence. In consultation with the Secretaries of State and Defense, the Director of Central Intelligence shall establish a comprehensive program for the periodic review of imagery from systems other than the Corona, Argon, and Lanyard missions, with the objective of making available to the public as much imagery as possible consistent with the interests of national defense and foreign policy. For imagery from obsolete broad-area film-return systems other than Corona, Argon, and Lanyard missions, this review shall be completed within 5 years of the date of this order. Review of imagery from any other system that the Director of Central Intelligence deems to be obsolete shall be accomplished according to a timetable established by the Director of Central Intelligence. The Director of Central Intelligence shall report annually to the President on the implementation of this order.
(b) The criteria referred to in section 2(a) of this order consist of the following: imagery acquired by a space-based national intelligence reconnaissance system other than the Corona, Argon, and Lanyard missions.

Sec. 3. General Provisions.

(a) This order prescribes a comprehensive and exclusive system for the public release of imagery acquired by space-based national intelligence reconnaissance systems. This order is the exclusive Executive order governing the public release of imagery for purposes of section 552(b)(1) of the Freedom of Information Act [5 U.S.C. 552(b)(1)].

(b) Nothing contained in this order shall create any right or benefit, substantive or procedural, enforceable by any party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

Sec. 4. Definition.

As used herein, “imagery” means the product acquired by space-based national intelligence reconnaissance systems that provides a likeness or representation of any natural or man-made feature or related objective or activities and satellite positional data acquired at the same time the likeness or representation was acquired.

William J. Clinton.
Executive Order 12968. Access to Classified Information

Ex. Ord. No. 12968, Aug. 2, 1995, 60 F.R. 40245, as amended by Ex. Ord. No. 13467, §3(b), June 30, 2008, 73 F.R. 38107, provided:

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS

Section 1.1. Definitions.

For the purposes of this order: (a) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105, the “military departments,” as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) “Applicant” means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) “Authorized investigative agency” means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain
whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) “Classified information” means information that has been determined pursuant to Executive Order No. 12958 [formerly set out above], or any successor order, Executive Order No. 12951 [set out above], or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 [et seq.]), to require protection against unauthorized disclosure.

(e) “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) “Foreign power” and “agent of a foreign power” have the meaning provided in 50 U.S.C. 1801.

(g) “Need for access” means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) “Need-to-know” means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) “Overseas Security Executive Agent” means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) “Security Executive Agent” means the Security Executive Agent established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) “Special access program” has the meaning provided in section 4.1 of Executive Order No. 12958 [formerly set out above], or any successor order.
Sec. 1.2. Access to Classified Information.

(a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee’s background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401[(6)]);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a [1681 et seq.]); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:
(A) there are reasonable grounds to believe, based on credible information, that
the employee or former employee is, or may be, disclosing classified information
in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or
former employee has incurred excessive indebtedness or has acquired a level of
affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability
and opportunity to disclose classified information that is known to have been lost
or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an
investigating agency to obtain information pursuant to the Right to Financial
U.S.C. 1681 et seq.] or any other applicable law.

Sec. 1.3. Financial Disclosure.

(a) Not later than 180 days after the effective date of this order, the head of each
agency that originates, handles, transmits, or possesses classified information
shall designate each employee, by position or category where possible, who has a
regular need for access to classified information that, in the discretion of the
agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection
Act of 1982 (50 U.S.C. 421 [et seq.]);

(2) technical or specialized national intelligence collection and processing
systems that, if disclosed in an unauthorized manner, would substantially negate
or impair the effectiveness of the system;

(3) the details of:

(A) the nature, contents, algorithm, preparation, or use of any code, cipher, or
cryptographic system or;

(B) the design, construction, functioning, maintenance, or repair of any
cryptographic equipment; but not including information concerning the use of
cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would
substantially negate or impair the effectiveness of the information or activity
involved; or
(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended [42 U.S.C. 2165(f)]).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Executive Agent.

(c) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Sec. 1.4. Use of Automated Financial Record Data Bases.

As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under $10,000 that are reported as possible money laundering violations, and records of foreign travel.

Sec. 1.5. Employee Education and Assistance.

The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to: (a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.
PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE

Sec. 2.1. Eligibility Determinations.

(a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Sec. 2.2. Level of Access Approval.

(a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.
(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Sec. 2.3. Temporary Access to Higher Levels.

(a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

(1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

(2) will not exceed 180 days; and

(3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

Sec. 2.4. Reciprocal Acceptance of Access Eligibility Determinations.

(a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.
(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Sec. 2.5. Specific Access Requirement.

(a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Sec. 2.6. Access by Non-United States Citizens.

(a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.
PART 3—ACCESS ELIGIBILITY STANDARDS

Sec. 3.1. Standards.

(a) No employee shall be deemed to be eligible for access to classified information merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in sections 2.6 and 3.3 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel or appropriate automated procedures. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.
Sec. 3.2. Basis for Eligibility Approval.

(a) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicant's or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

Sec. 3.3. Special Circumstances.

(a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Executive Agent not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.
(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years and who have been retired or otherwise separated from United States Government employment for not more than 2 years; provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

Sec. 3.4. Reinvestigation Requirements.

(a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

Sec. 3.5. Continuous Evaluation.

An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under
standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence.

PART 4—INVESTIGATIONS FOR FOREIGN GOVERNMENTS

Sec. 4. Authority.

Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

PART 5—REVIEW OF ACCESS DETERMINATIONS

Sec. 5.1. Determinations of Need for Access.

A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

Sec. 5.2. Review Proceedings for Denials or Revocations of Eligibility for Access.

(a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;
(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by subsection (a) of this section. This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) of this section cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f)(1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.
(2) Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) of this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

PART 6—IMPLEMENTATION

Sec. 6.1. Agency Implementing Responsibilities.

Heads of agencies that grant employees access to classified information shall: (a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Executive Agent, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Executive Agent.

Sec. 6.2. Employee Responsibilities.

(a) Employees who are granted eligibility for access to classified information shall:

(1) protect classified information in their custody from unauthorized disclosure;

(2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) report all violations of security regulations to the appropriate security officials; and

(4) comply with all other security requirements set forth in this order and its implementing regulations.
(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Sec. 6.3. Security Executive Agent Responsibilities and Implementation.

(a) With respect to actions taken by the Security Executive Agent pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Director of National Intelligence shall serve as the final authority for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Executive Agent pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Executive Agent shall consult where appropriate with the Overseas Security Executive Agent. In carrying out its responsibilities under section 1.3(c) of this order, the Security Executive Agent shall obtain the concurrence of the Director of the Office of Management and Budget.

Sec. 6.4. Sanctions.

Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

PART 7—GENERAL PROVISIONS

Sec. 7.1. Classified Information Procedures Act.

Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App.).

Sec. 7.2. General.

(a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

(1) the agency employing the employee who is the subject of the records or information;
(2) the Department of Justice for law enforcement or counterintelligence purposes; or

(3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450 [5 U.S.C. 7311 note], the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended [set out above], or access by historical researchers and former presidential appointees under Executive Order No. 12958 [formerly set out above] or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order is effective immediately.
Executive Order 13353. Establishing the President's Board on Safeguarding Americans’ Civil Liberties

Ex. Ord. No. 13353, Aug. 27, 2004, 69 F.R. 53585, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to further strengthen protections for the rights of Americans in the effective performance of national security and homeland security functions, it is hereby ordered as follows:

Section 1. Policy.

The United States Government has a solemn obligation, and shall continue fully, to protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions.

Sec. 2. Establishment of Board.

To advance the policy set forth in section 1 of this order (Policy), there is hereby established the President’s Board on Safeguarding Americans’ Civil Liberties (Board). The Board shall be part of the Department of Justice for administrative purposes.

Sec. 3. Functions.

The Board shall:

(a)(i) advise the President on effective means to implement the Policy, and (ii) keep the President informed of the implementation of the Policy;

(b) periodically request reports from Federal departments and agencies relating to policies and procedures that ensure implementation of the Policy;

(c) recommend to the President policies, guidelines and other administrative actions, technologies, and legislation, as necessary to implement the Policy;

(d) at the request of the head of any Federal department or agency, unless the Chair, after consultation with the Vice Chair, declines the request, promptly review and provide advice on a policy or action of that department or agency that implicates the Policy;

(e) obtain information and advice relating to the Policy from representatives of entities or individuals outside the executive branch of the Federal Government in
a manner that seeks their individual advice and does not involve collective judgment or consensus advice or deliberation;

(f) refer, consistent with section 535 of title 28, United States Code, credible information pertaining to possible violations of law relating to the Policy by any Federal employee or official to the appropriate office for prompt investigation;

(g) take steps to enhance cooperation and coordination among Federal departments and agencies in the implementation of the Policy, including but not limited to working with the Director of the Office of Management and Budget and other officers of the United States to review and assist in the coordination of guidelines and policies concerning national security and homeland security efforts, such as information collection and sharing; and

(h) undertake other efforts to protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, as the President may direct.

Upon the recommendation of the Board, the Attorney General or the Secretary of Homeland Security may establish one or more committees that include individuals from outside the executive branch of the Federal Government, in accordance with applicable law, to advise the Board on specific issues relating to the Policy. Any such committee shall carry out its functions separately from the Board.

**Sec. 4. Membership and Operation.**

The Board shall consist exclusively of the following:

(a) the Deputy Attorney General, who shall serve as Chair;

(b) the Under Secretary for Border and Transportation Security, Department of Homeland Security, who shall serve as Vice Chair;

(c) the Assistant Attorney General (Civil Rights Division);

(d) the Assistant Attorney General (Office of Legal Policy);

(e) the Counsel for Intelligence Policy, Department of Justice;

(f) the Chair of the Privacy Council, Federal Bureau of Investigation;

(g) the Assistant Secretary for Information Analysis, Department of Homeland Security;

---

*Page 126*
(h) the Assistant Secretary (Policy), Directorate of Border and Transportation Security, Department of Homeland Security;

(i) the Officer for Civil Rights and Civil Liberties, Department of Homeland Security;

(j) the Privacy Officer, Department of Homeland Security;

(k) the Under Secretary for Enforcement, Department of the Treasury;

(l) the Assistant Secretary (Terrorist Financing), Department of the Treasury;

(m) the General Counsel, Office of Management and Budget;

(n) the Deputy Director of Central Intelligence for Community Management;

(o) the General Counsel, Central Intelligence Agency;

(p) the General Counsel, National Security Agency;

(q) the Under Secretary of Defense for Intelligence;

(r) the General Counsel of the Department of Defense;

(s) the Legal Adviser, Department of State;

(t) the Director, Terrorist Threat Integration Center; and

(u) such other officers of the United States as the Deputy Attorney General may from time to time designate.

A member of the Board may designate, to perform the Board or Board subgroup functions of the member, any person who is part of such member’s department or agency and who is either (i) an officer of the United States appointed by the President, or (ii) a member of the Senior Executive Service or the Senior Intelligence Service. The Chair, after consultation with the Vice Chair, shall convene and preside at meetings of the Board, determine its agenda, direct its work, and, as appropriate to deal with particular subject matters, establish and direct subgroups of the Board that shall consist exclusively of members of the Board. The Chair may invite, in his discretion, officers or employees of other departments or agencies to participate in the work of the Board. The Chair shall convene the first meeting of the Board within 20 days after the date of this order and shall thereafter convene meetings of the Board at such times as the Chair, after consultation with the Vice Chair, deems appropriate. The Deputy Attorney
General shall designate an official of the Department of Justice to serve as the Executive Director of the Board.

**Sec. 5. Cooperation.**

To the extent permitted by law, all Federal departments and agencies shall cooperate with the Board and provide the Board with such information, support, and assistance as the Board, through the Chair, may request.

**Sec. 6. Administration.**

Consistent with applicable law and subject to the availability of appropriations, the Department of Justice shall provide the funding and administrative support for the Board necessary to implement this order.

**Sec. 7. General Provisions.**

(a) This order shall not be construed to impair or otherwise affect the authorities of any department, agency, instrumentality, officer, or employee of the United States under applicable law, including the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented in a manner consistent with applicable laws and Executive Orders concerning protection of information, including those for the protection of intelligence sources and methods, law enforcement information, and classified national security information, and the Privacy Act of 1974, as amended (5 U.S.C. 552a).

(c) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by a party against the United States, or any of its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any other person.

George W. Bush.
Executive Order 13434. National Security Professional Development

Ex. Ord. No. 13434, May 17, 2007, 72 F.R. 28583, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the national security, it is hereby ordered as follows:

Section 1. Policy.

In order to enhance the national security of the United States, including preventing, protecting against, responding to, and recovering from natural and manmade disasters, such as acts of terrorism, it is the policy of the United States to promote the education, training, and experience of current and future professionals in national security positions (security professionals) in executive departments and agencies (agencies).

Sec. 2. National Strategy for Professional Development.

Not later than 60 days after the date of this order, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT), in coordination with the Assistant to the President for National Security Affairs (APNSA), shall submit to the President for approval a National Strategy for the Development of Security Professionals (National Strategy). The National Strategy shall set forth a framework that will provide to security professionals access to integrated education, training, and professional experience opportunities for the purpose of enhancing their mission-related knowledge, skills, and experience and thereby improve their capability to safeguard the security of the Nation. Such opportunities shall be provided across organizations, levels of government, and incident management disciplines, as appropriate.

Sec. 3. Executive Steering Committee.

(a) There is established the Security Professional Development Executive Steering Committee (Steering Committee), which shall facilitate the implementation of the National Strategy. Not later than 120 days after the approval of the National Strategy by the President, the Steering Committee shall submit to the APHS/CT and the APNSA an implementation plan (plan) for the National Strategy, and annually thereafter shall submit to the APHS/CT and the APNSA a status report on the implementation of the plan and any recommendations for changes to the National Strategy.
(b) The Steering Committee shall consist exclusively of the following members (or their designees who shall be full-time officers or employees of the members’ respective agencies):

(i) the Director of the Office of Personnel Management, who shall serve as Chair;

(ii) the Secretary of State;

(iii) the Secretary of the Treasury;

(iv) the Secretary of Defense;

(v) the Attorney General;

(vi) the Secretary of Agriculture;

(vii) the Secretary of Labor;

(viii) the Secretary of Health and Human Services;

(ix) the Secretary of Housing and Urban Development;

(x) the Secretary of Transportation;

(xi) the Secretary of Energy;

(xii) the Secretary of Education;

(xiii) the Secretary of Homeland Security;

(xiv) the Director of National Intelligence;

(xv) the Director of the Office of Management and Budget; and

(xvi) such other officers of the United States as the Chair of the Steering Committee may designate from time to time.

(c) The Steering Committee shall coordinate, to the maximum extent practicable, national security professional development programs and guidance issued by the heads of agencies in order to ensure an integrated approach to such programs.

(d) The Chair of the Steering Committee shall convene and preside at the meetings of the Steering Committee, set its agenda, coordinate its work, and, as appropriate to deal with particular subject matters, establish subcommittees of the Steering Committee that shall consist exclusively of members of the Steering Committee.
Committee (or their designees under subsection (b) of this section), and such other full-time or permanent part-time officers or employees of the Federal Government as the Chair may designate.

**Sec. 4. Responsibilities.**

The head of each agency with national security functions shall:

(a) identify and enhance existing national security professional development programs and infrastructure, and establish new programs as necessary, in order to fulfill their respective missions to educate, train, and employ security professionals consistent with the National Strategy and, to the maximum extent practicable, the plan and related guidance from the Steering Committee; and

(b) cooperate with the Steering Committee and provide such information, support, and assistance as the Chair of the Steering Committee may request from time to time.

**Sec. 5. Additional Responsibilities.**

(a) Except for employees excluded by law, and subject to subsections (b), (c), and (d) of this section, the Director of the Office of Personnel Management, after consultation with the Steering Committee, shall:

(i) consistent with applicable merit-based hiring and advancement principles, lead the establishment of a national security professional development program in accordance with the National Strategy and the plan that provides for interagency and intergovernmental assignments and fellowship opportunities and provides for professional development guidelines for career advancement; and

(ii) issue to agencies rules and guidance or apply existing rules and guidance relating to the establishment of national security professional development programs to implement the National Strategy and the plan;

(b) The Secretary of Defense shall issue rules or guidance on professional development programs for Department of Defense military personnel, including interagency and intergovernmental assignments and fellowship opportunities, to implement the National Strategy and the plan, as appropriate, and shall coordinate such programs, to the maximum extent practicable, with the Steering Committee;

(c) The Secretary of State shall issue rules or guidance on national security professional development programs for the Foreign Service, including interagency and intergovernmental exchanges and fellowship opportunities, to
implement the National Strategy and the plan, as appropriate, and shall coordinate such programs, to the maximum extent practicable, with the Steering Committee;

(d) The Director of National Intelligence, in coordination with the heads of agencies of which elements of the intelligence community are a part, shall issue rules or guidance on national security professional development programs for the intelligence community, including interagency and intergovernmental assignments and fellowship opportunities, to implement the National Strategy and the plan, as appropriate, and shall coordinate such programs, to the maximum extent practicable, with the Steering Committee; and

(e) The Secretary of Homeland Security shall develop a program to provide to Federal, State, local, and tribal government officials education in disaster preparedness, response, and recovery plans and authorities, and training in crisis decision-making skills, consistent with applicable presidential guidance.

Sec. 6. General Provisions.

This order:

(a) shall be implemented consistent with applicable law and authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) shall not be construed to impair or otherwise affect the authorities of any agency, instrumentality, officer, or employee of the United States under applicable law, including the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals, or the functions assigned by the President to the Director of the Office of Personnel Management; and

(c) is not intended to, and does not, create any right, benefit, or privilege, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, instrumentalities, or entities, its officers or employees, or any other person.

George W. Bush.
Executive Order 13462. President's Intelligence Advisory Board and Intelligence Oversight Board


By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy.

It is the policy of the United States to ensure that the President and other officers of the United States with responsibility for the security of the Nation and the advancement of its interests have access to accurate, insightful, objective, and timely information concerning the capabilities, intentions, and activities of foreign powers.

Sec. 2. Definitions.

As used in this order:

(a) “department concerned” means an executive department listed in section 101 of title 5, United States Code, that contains an organization listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended (50 U.S.C. 401a(4));

(b) “intelligence activities” has the meaning specified in section 3.5 of Executive Order 12333 of December 4, 1981, as amended; and

(c) “intelligence community” means the organizations listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended.

Sec. 3. Establishment of the President's Intelligence Advisory Board.

(a) There is hereby established, within the Executive Office of the President and exclusively to advise and assist the President as set forth in this order, the President's Intelligence Advisory Board (PIAB).

(b) The PIAB shall consist of not more than 16 members appointed by the President from among individuals who are not full-time employees of the Federal Government.
(c) The President shall designate a Chair or Co-Chairs from among the members of the PIAB, who shall convene and preside at meetings of the PIAB, determine its agenda, and direct its work.

(d) Members of the PIAB and the Intelligence Oversight Board (IOB) established in section 5 of this order:

(i) shall serve without any compensation for their work on the PIAB or the IOB; and

(ii) while engaged in the work of the PIAB or the IOB, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government (5 U.S.C. 5701–5707).

(e) The PIAB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President’s designee. Such staff shall be supervised by an Executive Director of the PIAB, appointed by the President, whom the President may designate to serve also as the Executive Director of the IOB.

Sec. 4. Functions of the PIAB.

Consistent with the policy set forth in section 1 of this order, the PIAB shall have the authority to, as the PIAB determines appropriate, or shall, when directed by the President:

(a) assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, and of counterintelligence and other intelligence activities, assess the adequacy of management, personnel and organization in the intelligence community, and review the performance of all agencies of the Federal Government that are engaged in the collection, evaluation, or production of intelligence or the execution of intelligence policy and report the results of such assessments or reviews:

(i) to the President, as necessary but not less than twice each year; and

(ii) to the Director of National Intelligence (DNI) and the heads of departments concerned when the PIAB determines appropriate; and

(b) consider and make appropriate recommendations to the President, the DNI, or the head of the department concerned with respect to matters identified to the PIAB by the DNI or the head of a department concerned.
Sec. 5. Establishment of Intelligence Oversight Board.

(a) There is hereby established a committee of the PIAB to be known as the Intelligence Oversight Board.

(b) The IOB shall consist of not more than five members of the PIAB who are designated by the President from among members of the PIAB to serve on the IOB. The IOB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President's designee. Such staff shall be supervised by an Executive Director of the IOB, appointed by the President, whom the President may designate to serve also as the Executive Director of the PIAB.

(c) The President shall designate a Chair from among the members of the IOB, who shall convene and preside at meetings of the IOB, determine its agenda, and direct its work.

Sec. 6. Functions of the IOB.

Consistent with the policy set forth in section 1 of this order, the IOB shall:

(a) issue criteria on the thresholds for reporting matters to the IOB, to the extent consistent with section 1.6(c) of Executive Order 12333, as amended[,] or the corresponding provision of any successor order;

(b) inform the President of intelligence activities that the IOB believes:

(i)(A) may be unlawful or contrary to Executive Order or presidential directive; and

(B) are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or

(ii) should be immediately reported to the President[;]

(c) forward to the Attorney General information concerning intelligence activities that involve possible violations of Federal criminal laws or otherwise implicate the authority of the Attorney General;

(d) review and assess the effectiveness, efficiency, and sufficiency of the processes by which the DNI and the heads of departments concerned perform their respective functions under this order and report thereon as necessary, together with any recommendations, to the President and, as appropriate, the DNI and the head of the department concerned;
(e) receive and review information submitted by the DNI under subsection 7(c) of this order and make recommendations thereon, including for any needed corrective action, with respect to such information, and the intelligence activities to which the information relates, as necessary, but not less than twice each year, to the President, the DNI, and the head of the department concerned; and

(f) conduct, or request that the DNI or the head of the department concerned, as appropriate, carry out and report to the IOB the results of, investigations of intelligence activities that the IOB determines are necessary to enable the IOB to carry out its functions under this order.

Sec. 7. Functions of the Director of National Intelligence.

Consistent with the policy set forth in section 1 of this order, the DNI shall:

(a) with respect to guidelines applicable to organizations within the intelligence community that concern reporting of intelligence activities described in subsection 6(b)(i)(A) of this order:

(i) review and ensure that such guidelines are consistent with section 1.6(c) of Executive Order 12333, as amended, or a corresponding provision of any successor order, and this order; and

(ii) issue for incorporation in such guidelines instructions relating to the format and schedule of such reporting as necessary to implement this order;

(b) with respect to intelligence activities described in subsection 6(b)(i)(A) of this order:

(i) receive reports submitted to the IOB pursuant to section 1.6(c) of Executive Order 12333, as amended, or a corresponding provision of any successor order;

(ii) forward to the Attorney General information in such reports relating to such intelligence activities to the extent that such activities involve possible violations of Federal criminal laws or implicate the authority of the Attorney General unless the DNI or the head of the department concerned has previously provided such information to the Attorney General; and

(iii) monitor the intelligence community to ensure that the head of the department concerned has directed needed corrective actions and that such actions have been taken and report to the IOB and the head of the department concerned, and as appropriate the President, when such actions have not been timely taken; and
(c) submit to the IOB as necessary and no less than twice each year:

(i) an analysis of the reports received under subsection (b)(i) of this section, including an assessment of the gravity, frequency, trends, and patterns of occurrences of intelligence activities described in subsection 6(b)(i)(A) of this order;

(ii) a summary of direction under subsection (b)(iii) of this section and any related recommendations; and

(iii) an assessment of the effectiveness of corrective action taken by the DNI or the head of the department concerned with respect to intelligence activities described in subsection 6(b)(i)(A) of this order.

Sec. 8. Functions of Heads of Departments Concerned and Additional Functions of the Director of National Intelligence.

(a) To the extent permitted by law, the DNI and the heads of departments concerned shall provide such information and assistance as the PIAB and the IOB determine is needed to perform their functions under this order.

(b) The heads of departments concerned shall:

(i) ensure that the DNI receives:

(A) copies of reports submitted to the IOB pursuant to section 1.6(c) of Executive Order 12333, as amended, or a corresponding provision of any successor order; and

(B) such information and assistance as the DNI may need to perform functions under this order; and

(ii) designate the offices within their respective organizations that shall submit reports to the IOB required by Executive Order and inform the DNI and the IOB of such designations; and

(iii) ensure that departments concerned comply with instructions issued by the DNI under subsection 7(a)(ii) of this order.

(c) The head of a department concerned who does not implement a recommendation to that head of department from the PIAB under subsection 4(b) of this order or from the IOB under subsections 6(c) or 6(d) of this order shall promptly report through the DNI to the Board that made the
recommendation, or to the President, the reasons for not implementing the recommendation.

(d) The DNI shall ensure that the Director of the Central Intelligence Agency performs the functions with respect to the Central Intelligence Agency under this order that a head of a department concerned performs with respect to organizations within the intelligence community that are part of that department.

Sec. 9. References and Transition.

(a) References in Executive Orders other than this order, or in any other presidential guidance, to the “President's Foreign Intelligence Advisory Board” shall be deemed to be references to the President's Intelligence Advisory Board established by this order.

(b) Individuals who are members of the President's Foreign Intelligence Advisory Board under Executive Order 12863 of September 13, 1993, as amended, immediately prior to the signing of this order shall be members of the President's Intelligence Advisory Board immediately upon the signing of this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.

(c) Individuals who are members of the Intelligence Oversight Board under Executive Order 12863 immediately prior to the signing of this order shall be members of the Intelligence Oversight Board under this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.

(d) The individual serving as Executive Director of the President's Foreign Intelligence Advisory Board immediately prior to the signing of this order shall serve as the Executive Director of the PIAB until such person resigns, dies, or is removed, or upon appointment of a successor under this order and shall serve as the Executive Director of the IOB until an Executive Director of the IOB is appointed or designated under this order.

Sec. 10. Revocation.

Executive Order 12863 is revoked.

Sec. 11. General Provisions.

(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) authority granted by law to a department or agency, or the head thereof; or
(ii) functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) Any person who is a member of the PIAB or the IOB, or who is granted access to classified national security information in relation to the activities of the PIAB or the IOB, as a condition of access to such information, shall sign and comply with appropriate agreements to protect such information from unauthorized disclosure. This order shall be implemented in a manner consistent with Executive Order 12958 of April 17, 1995, as amended, and Executive Order 12968 of August 2, 1995, as amended.

(c) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(d) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

George W. Bush.
Effective Dates of Provisions in Title I of the Intelligence Reform and Terrorism Prevention Act of 2004

Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, provided:

Memorandum for the Secretary of State[, the Secretary of the Treasury[, the Secretary of Defense[,[ the Attorney General[,] the Secretary of Energy[,] the Secretary of Homeland Security[,] the Director of the Office of Management and Budget[, and] the Director of National Intelligence

Subsection 1097(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458, December 17, 2004) (the Act) [set out in a note above] provides:

(a) IN GENERAL- Except as otherwise expressly provided in this Act, this title and the amendments made by this title shall take effect not later than 6 months after the date of enactment of this Act.

Subsection 1097(a) clearly contemplates that one or more of the provisions in Title I of the Act may take effect earlier than the date that is 6 months after the date of enactment of the Act, but does not state explicitly the mechanism for determining when such earlier effect shall occur, leaving it to the President in the execution of the Act. Moreover, given that section 1097(a) evinces a legislative intent to afford the President flexibility, and such flexibility is constitutionally appropriate with respect to intelligence matters (see United States v. Curtiss-Wright Export Corporation, 299 U.S. 304 (1936)), the executive branch shall construe section 1097(a) to authorize the President to select different effective dates that precede the 6-month deadline for different provisions in Title I.

Therefore, pursuant to the Constitution and the laws of the United States of America, including subsection 1097(a) of the Act, I hereby determine and direct:

1. Sections 1097(a) and 1103 of the Act [set out in notes above], relating respectively to effective dates of provisions and to severability, shall take effect immediately upon the signing of this memorandum to any extent that they have not already taken effect.

2. Provisions in Title I of the Act other than those addressed in numbered paragraph 1 of this memorandum shall take effect immediately upon the signing of this memorandum, except:
(a) any provision in Title I of the Act for which the Act expressly provides the date on which the provision shall take effect; and

(b) sections 1021 and 1092 of the Act [enacting section 4040 of this title and provisions set out in a note above, respectively], relating to the National Counterterrorism Center.

The taking of effect of a provision pursuant to section 1097(a) of the Act and this memorandum shall not affect the construction of such provision by the executive branch as set forth in my Statement of December 17, 2004, upon signing the Act into law.

The Director of the Office of Management and Budget is authorized and directed to publish this memorandum in the Federal Register.

George W. Bush.
Executive Order 13467. Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information

Ex. Ord. No. 13467, June 30, 2008, 73 F.R. 38103, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Government employment, contractor employee fitness, and eligibility for access to classified information, while taking appropriate account of title III of Public Law 108–458, it is hereby ordered as follows:

PART 1—POLICY, APPLICABILITY, AND DEFINITIONS

Section 1.1. Policy.

Executive branch policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation’s business and protect national security.

Sec. 1.2. Applicability.

(a) This order applies to all covered individuals as defined in section 1.3(g), except that:

(i) the provisions regarding eligibility for physical access to federally controlled facilities and logical access to federally controlled information systems do not apply to individuals exempted in accordance with guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107–347) and Homeland Security Presidential Directive 12; and

(ii) the qualification standards for enlistment, appointment, and induction into the Armed Forces pursuant to title 10, United States Code, are unaffected by this order.

(b) This order also applies to investigations and determinations of eligibility for access to classified information for employees of agencies working in or for the
legislative or judicial branches when those investigations or determinations are conducted by the executive branch.

Sec. 1.3. Definitions.

For the purpose of this order: (a) “Adjudication” means the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is:

(i) suitable for Government employment;

(ii) eligible for logical and physical access;

(iii) eligible for access to classified information;

(iv) eligible to hold a sensitive position; or

(v) fit to perform work for or on behalf of the Government as a contractor employee.

(b) “Agency” means any “Executive agency” as defined in section 105 of title 5, United States Code, including the “military departments,” as defined in section 102 of title 5, United States Code, and any other entity within the executive branch that comes into possession of classified information or has designated positions as sensitive, except such an entity headed by an officer who is not a covered individual.

(c) “Classified information” means information that has been determined pursuant to Executive Order 12958 of April 17, 1995, as amended, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

(d) “Continuous evaluation” means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.

(e) “Contractor” means an expert or consultant (not appointed under section 3109 of title 5, United States Code) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all
subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).

(f) “Contractor employee fitness” means fitness based on character and conduct for work for or on behalf of the Government as a contractor employee.

(g) “Covered individual” means a person who performs work for or on behalf of the executive branch, or who seeks to perform work for or on behalf of the executive branch, but does not include:

(i) the President or (except to the extent otherwise directed by the President) employees of the President under section 105 or 107 of title 3, United States Code; or

(ii) the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under section 106 of title 3 or annual legislative branch appropriations acts.

(h) “End-to-end automation” means an executive branch-wide federated system that uses automation to manage and monitor cases and maintain relevant documentation of the application (but not an employment application), investigation, adjudication, and continuous evaluation processes.

(i) “Federally controlled facilities” and “federally controlled information systems” have the meanings prescribed in guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107–347) and Homeland Security Presidential Directive 12.

(j) “Logical and physical access” means access other than occasional or intermittent access to federally controlled facilities or information systems.

(k) “Sensitive position” means any position so designated under Executive Order 10450 of April 27, 1953, as amended.

(l) “Suitability” has the meaning and coverage provided in 5 CFR Part 731.

PART 2—ALIGNMENT, RECIPROCITY, AND GOVERNANCE

Sec. 2.1. Aligned System.

(a) Investigations and adjudications of covered individuals who require a determination of suitability, eligibility for logical and physical access, eligibility to hold a sensitive position, eligibility for access to classified information, and, as appropriate, contractor employee fitness, shall be aligned using consistent
standards to the extent possible. Each successively higher level of investigation and adjudication shall build upon, but not duplicate, the ones below it.

(b) The aligned system shall employ updated and consistent standards and methods, enable innovations with enterprise information technology capabilities and end-to-end automation to the extent practicable, and ensure that relevant information maintained by agencies can be accessed and shared rapidly across the executive branch, while protecting national security, protecting privacy-related information, ensuring resulting decisions are in the national interest, and providing the Federal Government with an effective workforce.

(c) Except as otherwise authorized by law, background investigations and adjudications shall be mutually and reciprocally accepted by all agencies. An agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination consistent with law, directive, or regulation) that exceed the requirements for suitability, contractor employee fitness, eligibility for logical or physical access, eligibility to hold a sensitive position, or eligibility for access to classified information without the approval of the Suitability Executive Agent or Security Executive Agent, as appropriate, and provided that approval to establish additional requirements shall be limited to circumstances where additional requirements are necessary to address significant needs unique to the agency involved or to protect national security.

Sec. 2.2. Establishment and Functions of Performance Accountability Council.

(a) There is hereby established a Suitability and Security Clearance Performance Accountability Council (Council).

(b) The Deputy Director for Management, Office of Management and Budget, shall serve as Chair of the Council and shall have authority, direction, and control over the Council's functions. Membership on the Council shall include the Suitability Executive Agent and the Security Executive Agent. The Chair shall select a Vice Chair to act in the Chair's absence. The Chair shall have authority to designate officials from additional agencies who shall serve as members of the Council. Council membership shall be limited to Federal Government employees and shall include suitability and security professionals.

(c) The Council shall be accountable to the President to achieve, consistent with this order, the goals of reform, and is responsible for driving implementation of the reform effort, ensuring accountability by agencies, ensuring the Suitability Executive Agent and the Security Executive Agent align their respective processes, and sustaining reform momentum.
(d) The Council shall:

(i) ensure alignment of suitability, security, and, as appropriate, contractor employee fitness investigative and adjudicative processes;

(ii) hold agencies accountable for the implementation of suitability, security, and, as appropriate, contractor employee fitness processes and procedures;

(iii) establish requirements for enterprise information technology;

(iv) establish annual goals and progress metrics and prepare annual reports on results;

(v) ensure and oversee the development of tools and techniques for enhancing background investigations and the making of eligibility determinations;

(vi) arbitrate disparities in procedures between the Suitability Executive Agent and the Security Executive Agent;

(vii) ensure sharing of best practices; and

(viii) advise the Suitability Executive Agent and the Security Executive Agent on policies affecting the alignment of investigations and adjudications.

(e) The Chair may, to ensure the effective implementation of the policy set forth in section 1.1 of this order and to the extent consistent with law, assign, in whole or in part, to the head of any agency (solely or jointly) any function within the Council’s responsibility relating to alignment and improvement of investigations and determinations of suitability, contractor employee fitness, eligibility for logical and physical access, eligibility for access to classified information, or eligibility to hold a sensitive position.

Sec. 2.3. Establishment, Designation, and Functions of Executive Agents.

(a) There is hereby established a Suitability Executive Agent and a Security Executive Agent.

(b) The Director of the Office of Personnel Management shall serve as the Suitability Executive Agent. As the Suitability Executive Agent, the Director of the Office of Personnel Management will continue to be responsible for developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access.
(c) The Director of National Intelligence shall serve as the Security Executive Agent. The Security Executive Agent:

(i) shall direct the oversight of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position made by any agency;

(ii) shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position;

(iii) may issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position;

(iv) shall serve as the final authority to designate an agency or agencies to conduct investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position;

(v) shall serve as the final authority to designate an agency or agencies to determine eligibility for access to classified information in accordance with Executive Order 12968 of August 2, 1995;

(vi) shall ensure reciprocal recognition of eligibility for access to classified information among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position; and

(vii) may assign, in whole or in part, to the head of any agency (solely or jointly) any of the functions detailed in (i) through (vi), above, with the agency's exercise of such assigned functions to be subject to the Security Executive Agent’s oversight and with such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate.

(d) Nothing in this order shall be construed in a manner that would limit the authorities of the Director of the Office of Personnel Management or the Director of National Intelligence under law.
Sec. 2.4. Additional Functions.

(a) The duties assigned to the Security Policy Board by Executive Order 12968 of August 2, 1995, to consider, coordinate, and recommend policy directives for executive branch security policies, procedures, and practices are reassigned to the Security Executive Agent.

(b) Heads of agencies shall:

(i) carry out any function assigned to the agency head by the Chair, and shall assist the Chair, the Council, the Suitability Executive Agent, and the Security Executive Agent in carrying out any function under sections 2.2 and 2.3 of this order;

(ii) implement any policy or procedure developed pursuant to this order;

(iii) to the extent permitted by law, make available to the Performance Accountability Council, the Suitability Executive Agent, or the Security Executive Agent such information as may be requested to implement this order;

(iv) ensure that all actions taken under this order take account of the counterintelligence interests of the United States, as appropriate; and

(v) ensure that actions taken under this order are consistent with the President’s constitutional authority to:

(A) conduct the foreign affairs of the United States;

(B) withhold information the disclosure of which could impair the foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive’s constitutional duties;

(C) recommend for congressional consideration such measures as the President may judge necessary or expedient; and

(D) supervise the unitary executive branch.

PART 3—MISCELLANEOUS

Sec. 3. General Provisions.

(a) Executive Order 13381 of June 27, 2005, as amended, is revoked. Nothing in this order shall:

(i) supersede, impede, or otherwise affect:
(A) Executive Order 10450 of April 27, 1953, as amended;

(B) Executive Order 10577 of November 23, 1954, as amended;

(C) Executive Order 12333 of December 4, 1981, as amended;

(D) Executive Order 12829 of January 6, 1993, as amended; or

(E) Executive Order 12958 of April 17, 1995, as amended; nor

(ii) diminish or otherwise affect the denial and revocation procedures provided to
individuals covered by Executive Order 10865 of February 20, 1960, as amended.

(b) [Amended Ex. Ord. No. 12968, set out above.]

(c) Nothing in this order shall supersede, impede, or otherwise affect the
remainder of Executive Order 12968 of August 2, 1995, as amended.

(d) [Amended Ex. Ord. No. 12171, set out as a note under section 7103 of Title 5,
Government Organization and Employees.]

(e) Nothing in this order shall be construed to impair or otherwise affect the:

(i) authority granted by law to a department or agency, or the head thereof; or

(ii) functions of the Director of the Office of Management and Budget relating to
budget, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to
the availability of appropriations.

(g) Existing delegations of authority made pursuant to Executive Order 13381 of
June 27, 2005, as amended, to any agency relating to granting eligibility for
access to classified information and conducting investigations shall remain in effect, subject to the exercise of authorities pursuant to this order to
revise or revoke such delegation.

(h) If any provision of this order or the application of such provision is held to be
invalid, the remainder of this order shall not be affected.

(i) This order is intended only to improve the internal management of the
executive branch and is not intended to, and does not, create any right or benefit,
substantive or procedural, enforceable at law or in equity, by any party against
the United States, its agencies, instrumentalities, or entities, its officers or
employees, or any other person.
George W. Bush.
Executive Order 13491. Ensuring Lawful Interrogations

Ex. Ord. No. 13491, Jan. 22, 2009, 74 F.R. 4893, provided:

By the authority vested in me by the Constitution and the laws of the United States of America, in order to improve the effectiveness of human intelligence-gathering, to promote the safe, lawful, and humane treatment of individuals in United States custody and of United States personnel who are detained in armed conflicts, to ensure compliance with the treaty obligations of the United States, including the Geneva Conventions, and to take care that the laws of the United States are faithfully executed, I hereby order as follows:

Section 1. Revocation.

Executive Order 13440 of July 20, 2007, is revoked. All executive directives, orders, and regulations inconsistent with this order, including but not limited to those issued to or by the Central Intelligence Agency (CIA) from September 11, 2001, to January 20, 2009, concerning detention or the interrogation of detained individuals, are revoked to the extent of their inconsistency with this order. Heads of departments and agencies shall take all necessary steps to ensure that all directives, orders, and regulations of their respective departments or agencies are consistent with this order. Upon request, the Attorney General shall provide guidance about which directives, orders, and regulations are inconsistent with this order.

Sec. 2. Definitions.

As used in this order:


(c) “Common Article 3” means Article 3 of each of the Geneva Conventions.


(e) “Geneva Conventions” means:
(i) the Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949 (6 UST 3114);

(ii) the Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, August 12, 1949 (6 UST 3217);

(iii) the Convention Relative to the Treatment of Prisoners of War, August 12, 1949 (6 UST 3316); and

(iv) the Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949 (6 UST 3516).

(f) “Treated humanely,” “violence to life and person,” “murder of all kinds,” “mutilation,” “cruel treatment,” “torture,” “outrages upon personal dignity,” and “humiliating and degrading treatment” refer to, and have the same meaning as, those same terms in Common Article 3.

(g) The terms “detention facilities” and “detention facility” in section 4(a) of this order do not refer to facilities used only to hold people on a short-term, transitory basis.

Sec. 3. Standards and Practices for Interrogation of Individuals in the Custody or Control of the United States in Armed Conflicts.

(a) Common Article 3 Standards as a Minimum Baseline. Consistent with the requirements of the Federal torture statute, 18 U.S.C. 2340–2340A, section 1003 of the Detainee Treatment Act of 2005, 42 U.S.C. 2000dd, the Convention Against Torture, Common Article 3, and other laws regulating the treatment and interrogation of individuals detained in any armed conflict, such persons shall in all circumstances be treated humanely and shall not be subjected to violence to life and person (including murder of all kinds, mutilation, cruel treatment, and torture), nor to outrages upon personal dignity (including humiliating and degrading treatment), whenever such individuals are in the custody or under the effective control of an officer, employee, or other agent of the United States Government or detained within a facility owned, operated, or controlled by a department or agency of the United States.

(b) Interrogation Techniques and Interrogation-Related Treatment. Effective immediately, an individual in the custody or under the effective control of an officer, employee, or other agent of the United States Government, or detained within a facility owned, operated, or controlled by a department or agency of the United States, in any armed conflict, shall not be subjected to any interrogation technique or approach, or any treatment related to interrogation, that is not authorized by and listed in Army Field Manual 2–22.3 (Manual). Interrogation
techniques, approaches, and treatments described in the Manual shall be implemented strictly in accord with the principles, processes, conditions, and limitations the Manual prescribes. Where processes required by the Manual, such as a requirement of approval by specified Department of Defense officials, are inapposite to a department or an agency other than the Department of Defense, such a department or agency shall use processes that are substantially equivalent to the processes the Manual prescribes for the Department of Defense. Nothing in this section shall preclude the Federal Bureau of Investigation, or other Federal law enforcement agencies, from continuing to use authorized, non-coercive techniques of interrogation that are designed to elicit voluntary statements and do not involve the use of force, threats, or promises.


Sec. 4. Prohibition of Certain Detention Facilities, and Red Cross Access to Detained Individuals.

(a) CIA Detention. The CIA shall close as expeditiously as possible any detention facilities that it currently operates and shall not operate any such detention facility in the future.

(b) International Committee of the Red Cross Access to Detained Individuals. All departments and agencies of the Federal Government shall provide the International Committee of the Red Cross with notification of, and timely access to, any individual detained in any armed conflict in the custody or under the effective control of an officer, employee, or other agent of the United States Government or detained within a facility owned, operated, or controlled by a department or agency of the United States Government, consistent with Department of Defense regulations and policies.

Sec. 5. Special Interagency Task Force on Interrogation and Transfer Policies.

(a) Establishment of Special Interagency Task Force. There shall be established a Special Task Force on Interrogation and Transfer Policies (Special Task Force) to review interrogation and transfer policies.
(b) **Membership.** The Special Task Force shall consist of the following members, or their designees:

(i) the Attorney General, who shall serve as Chair;

(ii) the Director of National Intelligence, who shall serve as Co-Vice-Chair;

(iii) the Secretary of Defense, who shall serve as Co-Vice-Chair;

(iv) the Secretary of State;

(v) the Secretary of Homeland Security;

(vi) the Director of the Central Intelligence Agency;

(vii) the Chairman of the Joint Chiefs of Staff; and

(viii) other officers or full-time or permanent part-time employees of the United States, as determined by the Chair, with the concurrence of the head of the department or agency concerned.

(c) **Staff.** The Chair may designate officers and employees within the Department of Justice to serve as staff to support the Special Task Force. At the request of the Chair, officers and employees from other departments or agencies may serve on the Special Task Force with the concurrence of the head of the department or agency that employ such individuals. Such staff must be officers or full-time or permanent part-time employees of the United States. The Chair shall designate an officer or employee of the Department of Justice to serve as the Executive Secretary of the Special Task Force.

(d) **Operation.** The Chair shall convene meetings of the Special Task Force, determine its agenda, and direct its work. The Chair may establish and direct subgroups of the Special Task Force, consisting exclusively of members of the Special Task Force, to deal with particular subjects.

(e) **Mission.** The mission of the Special Task Force shall be:

(i) to study and evaluate whether the interrogation practices and techniques in Army Field Manual 2–22.3, when employed by departments or agencies outside the military, provide an appropriate means of acquiring the intelligence necessary to protect the Nation, and, if warranted, to recommend any additional or different guidance for other departments or agencies; and

(ii) to study and evaluate the practices of transferring individuals to other nations in order to ensure that such practices comply with the domestic laws,
international obligations, and policies of the United States and do not result in the transfer of individuals to other nations to face torture or otherwise for the purpose, or with the effect, of undermining or circumventing the commitments or obligations of the United States to ensure the humane treatment of individuals in its custody or control.

(f) Administration. The Special Task Force shall be established for administrative purposes within the Department of Justice and the Department of Justice shall, to the extent permitted by law and subject to the availability of appropriations, provide administrative support and funding for the Special Task Force.

(g) Recommendations. The Special Task Force shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Counsel to the President, on the matters set forth in subsection (d) within 180 days of the date of this order, unless the Chair determines that an extension is necessary.

(h) Termination. The Chair shall terminate the Special Task Force upon the completion of its duties.

Sec. 6. Construction with Other Laws.

Nothing in this order shall be construed to affect the obligations of officers, employees, and other agents of the United States Government to comply with all pertinent laws and treaties of the United States governing detention and interrogation, including but not limited to: the Fifth and Eighth Amendments to the United States Constitution; the Federal torture statute, 18 U.S.C. 2340–2340A; the War Crimes Act [of 1996], 18 U.S.C. 2441; the Federal assault statute, 18 U.S.C. 113; the Federal maiming statute, 18 U.S.C. 114; the Federal “stalking” statute, 18 U.S.C. 2261A; articles 93, 124, 128, and 134 of the Uniform Code of Military Justice, 10 U.S.C. 893, 924, 928, and 934; section 1003 of the Detainee Treatment Act of 2005, 42 U.S.C. 2000dd; section 6(c) of the Military Commissions Act of 2006, Public Law 109–366; the Geneva Conventions; and the Convention Against Torture. Nothing in this order shall be construed to diminish any rights that any individual may have under these or other laws and treaties. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

Barack Obama.
Executive Order 13526. Classified National Security Information

Ex. Ord. No. 13526, Dec. 29, 2009, 75 F.R. 707, 1013, provided:

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—Original Classification

Section 1.1. Classification Standards.

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:
(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. Classification Levels.

(a) Information may be classified at one of the following three levels:

(1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.3. Classification Authority.

(a) The authority to classify information originally may be exercised only by:

(1) the President and the Vice President;

(2) agency heads and officials designated by the President; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.
(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) “Top Secret” original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) “Secret” or “Confidential” original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated “Top Secret” original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.
(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information.

**Sec. 1.4. Classification Categories.**

Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or (h) the development, production, or use of weapons of mass destruction.

**Sec. 1.5. Duration of Classification.**

(a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts
of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as “Originating Agency's Determination Required,” or classified information that contains incomplete declassification instructions or lacks declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.6. Identification and Markings.

(a) At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name and position, or by personal identifier, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or
(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant and revoke temporary waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.
(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. Classification Prohibitions and Limitations.

(a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may not be reclassified after declassification and release to the public under proper authority unless:

(1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;

(2) the information may be reasonably recovered without bringing undue attention to the information;

(3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.
(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

Sec. 1.8. Classification Challenges.

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.
(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

Sec. 1.9. Fundamental Classification Guidance Review.

(a) Agency heads shall complete on a periodic basis a comprehensive review of the agency’s classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

PART 2—Derivative Classification

Sec. 2.1. Use of Derivative Classification.

(a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:
(A) the date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

**Sec. 2.2. Classification Guides.**

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.
(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides, provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

1. information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and

2. specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

PART 3—Declassification and Downgrading

Sec. 3.1. Authority for Declassification.

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

1. the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;

2. the originator's current successor in function, if that individual has original classification authority;

3. a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or (4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be
outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(e) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

Sec. 3.2. Transferred Records.

(a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.
(c) Classified records accessioned into the National Archives shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

Sec. 3.3 Automatic Declassification.

(a) Subject to paragraphs (b)–(d) and (g)–(j) of this section, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(j) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

(1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;
(4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.

(2) The notification shall include:

(A) a description of the file series;

(B) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than
recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declassification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.
(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.
(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(B) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.
Sec. 3.4. Systematic Declassification Review.

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records:

(1) accessioned into the National Archives; (2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

Sec. 3.5. Mandatory Declassification Review.

(a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent President’s White House Staff or the incumbent Vice President’s Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records.
Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(f) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of National Intelligence shall develop special procedures for the review of information pertaining to intelligence sources, methods, and activities; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

Sec. 3.6. Processing Requests and Reviews.

Notwithstanding section 4.1(i) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:
(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

(1) the specific information has been approved pursuant to section 3.3(j) of this order for exemption from automatic declassification; and

(2) the extension does not exceed the date established in section 3.3(j) of this order.

Sec. 3.7. National Declassification Center.

(a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

(1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.

(2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;
(3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;

(4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;

(5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;

(6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and

(7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

(1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and

(2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt or declassify information originated by their agency contained in records accessioned into the National Archives, after consultation with subject-matter experts as necessary.

(d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.

(e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that relate to records determined to have permanent historical value.

(f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence,
Director shall also retain such authority with respect to the Intelligence Community.

(g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

PART 4—Safeguarding

Sec. 4.1. General Restrictions on Access.

(a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) An official or employee leaving agency service may not remove classified information from the agency’s control or direct that information be declassified in order to remove it from agency control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, shall establish uniform procedures to ensure that automated information systems, including networks and
telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:

(1) prevent access by unauthorized persons;

(2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

(A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. “Confidential” information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction
of the President, or with the consent of the originating agency. For the purposes of this section, "foreign government" includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

Sec. 4.2 Distribution Controls.

(a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information (including information marked pursuant to section 4.1(i)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution mechanism for classified information that it distributes.
Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.3. Special Access Programs.

(a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations.

(1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director of the Information Security Oversight Office and no more than one other employee of the Information Security Oversight Office or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.
(5) Upon request, an agency head shall brief the National Security Advisor, or a designee, on any or all of the agency’s special access programs.

(6) For the purposes of this section, the term “agency head” refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel.

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or

(3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

PART 5—Implementation and Review

Sec. 5.1. Program Direction.

(a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue
such directives as are necessary to implement this order. These directives shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification, declassification, and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

Sec. 5.2. Information Security Oversight Office.

(a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and
information and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the National Security Advisor;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.3. Interagency Security Classification Appeals Panel.

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

Sec. 5.3. Interagency Security Classification Appeals Panel.
(4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(6) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(7) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and

(4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the Federal Register. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the Federal courts; and

(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the
President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

Sec. 5.4. General Responsibilities.

Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of
this order; and reporting annually to the Director of the Information Security Oversight Office on the agency’s self-inspection program;

(5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information be established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.
Sec. 5.5. Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

PART 6—General Provisions

Sec. 6.1. Definitions.

For purposes of this order:
(a) “Access” means the ability or opportunity to gain knowledge of classified information.

(b) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) “Authorized holder” of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.

(d) “Automated information system” means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) “Automatic declassification” means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(f) “Classification” means the act or process by which information is determined to be classified information.

(g) “Classification guidance” means any instruction or source that prescribes the classification of specific information.

(h) “Classification guide” means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(i) “Classified national security information” or “classified information” means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(j) “Compilation” means an aggregation of preexisting unclassified items of information.

(k) “Confidential source” means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States
on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) “Damage to the national security” means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) “Declassification” means the authorized change in the status of information from classified information to unclassified information.

(n) “Declassification guide” means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(o) “Derivative classification” means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(p) “Document” means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) “Downgrading” means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) “File series” means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) “Foreign government information” means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an
international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as “foreign government information” under the terms of a predecessor order.

(t) “Information” means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

(u) “Infraction” means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a “violation,” as defined below.

(v) “Integral file block” means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

(w) “Integrity” means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(x) “Intelligence” includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) “Intelligence activities” means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) “Intelligence Community” means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) “Mandatory declassification review” means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.
(bb) “Multiple sources” means two or more source documents, classification guides, or a combination of both.

(cc) “National security” means the national defense or foreign relations of the United States.

(dd) “Need-to-know” means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) “Network” means a system of two or more computers that can exchange data or information.

(ff) “Original classification” means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) “Original classification authority” means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(hh) “Records” means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency’s control under the terms of the contract, license, certificate, or grant.

(ii) “Records having permanent historical value” means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) “Records management” means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) “Safeguarding” means measures and controls that are prescribed to protect classified information.
(II) “Self-inspection” means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) “Senior agency official” means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency’s program under which information is classified, safeguarded, and declassified.

(nn) “Source document” means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) “Special access program” means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) “Systematic declassification review” means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) “Telecommunications” means the preparation, transmission, or communication of information by electronic means.

(rr) “Unauthorized disclosure” means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) “U.S. entity” includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) “Violation” means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) “Weapons of mass destruction” means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

Sec. 6.2. General Provisions.

(a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. “Restricted Data” and “Formerly Restricted Data” shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. The foregoing is in addition to the specific provisos set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.
(e) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

   Sec. 6.3. Effective Date.

This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

   Sec. 6.4. Publication.

The Archivist of the United States shall publish this Executive Order in the Federal Register.

Barack Obama.
**Executive Order 13549. Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities**

Ex. Ord. No. 13549, Aug. 18, 2010, 75 F.R. 51609, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, in order to ensure the proper safeguarding of information shared with State, local, tribal, and private sector entities, it is hereby ordered as follows:

**Section 1. Establishment and Policy.**

Sec. 1.1. There is established a Classified National Security Information Program (Program) designed to safeguard and govern access to classified national security information shared by the Federal Government with State, local, tribal, and private sector (SLTPS) entities.

Sec. 1.2. The purpose of this order is to ensure that security standards governing access to and safeguarding of classified material are applied in accordance with Executive Order 13526 of December 29, 2009 (“Classified National Security Information”), Executive Order 12968 of August 2, 1995, as amended (“Access to Classified Information”), Executive Order 13467 of June 30, 2008 (“Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information”), and Executive Order 12829 of January 6, 1993, as amended (“National Industrial Security Program”). Procedures for uniform implementation of these standards by SLTPS entities shall be set forth in an implementing directive to be issued by the Secretary of Homeland Security within 180 days of the date of this order, in consultation with affected executive departments and agencies (agencies), and with the concurrence of the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the Director of the Information Security Oversight Office.

Sec. 1.3. Additional policy provisions for access to and safeguarding of classified information shared with SLTPS personnel include the following:

(a) Eligibility for access to classified information by SLTPS personnel shall be determined by a sponsoring agency. The level of access granted shall not exceed the Secret level, unless the sponsoring agency determines on a case-by-case basis that the applicant has a demonstrated and foreseeable need for access to Top Secret, Special Access Program, or Sensitive Compartmented Information.
(b) Upon the execution of a non-disclosure agreement prescribed by the Information Security Oversight Office or the Director of National Intelligence, and absent disqualifying conduct as determined by the clearance granting official, a duly elected or appointed Governor of a State or territory, or an official who has succeeded to that office under applicable law, may be granted access to classified information without a background investigation in accordance with the implementing directive for this order. This authorization of access may not be further delegated by the Governor to any other person.

(c) All clearances granted to SLTPS personnel, as well as accreditations granted to SLTPS facilities without a waiver, shall be accepted reciprocally by all agencies and SLTPS entities.

(d) Physical custody of classified information by State, local, and tribal (SLT) entities shall be limited to Secret information unless the location housing the information is under the full-time management, control, and operation of the Department of Homeland Security or another agency. A standard security agreement, established by the Department of Homeland Security in consultation with the SLTPS Advisory Committee, shall be executed between the head of the SLT entity and the U.S. Government for those locations where the SLT entity will maintain physical custody of classified information.

(e) State, local, and tribal facilities where classified information is or will be used or stored shall be inspected, accredited, and monitored for compliance with established standards, in accordance with Executive Order 13526 and the implementing directive for this order, by the Department of Homeland Security or another agency that has entered into an agreement with the Department of Homeland Security to perform such inspection, accreditation, and monitoring.

(f) Private sector facilities where classified information is or will be used or stored shall be inspected, accredited, and monitored for compliance with standards established pursuant to Executive Order 12829, as amended, by the Department of Defense or the cognizant security agency under Executive Order 12829, as amended.

(g) Access to information systems that store, process, or transmit classified information shall be enforced by the rules established by the agency that controls the system and consistent with approved dissemination and handling markings applied by originators, separate from and in addition to criteria for determining eligibility for access to classified information. Access to information within restricted portals shall be based on criteria applied by the agency that controls the portal and consistent with approved dissemination and handling markings applied by originators.

(h) The National Industrial Security Program established in Executive Order 12829, as amended, shall govern the access to and safeguarding of classified
information that is released to contractors, licensees, and grantees of SLT entities.

(i) All access eligibility determinations and facility security accreditations granted prior to the date of this order that do not meet the standards set forth in this order or its implementing directive shall be reconciled with those standards within a reasonable period.

(j) Pursuant to section 4.1(i)(3) of Executive Order 13526, documents created prior to the effective date of Executive Order 13526 shall not be re-disseminated to other entities without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

Sec. 2. Policy Direction.

With policy guidance from the National Security Advisor and in consultation with the Director of the Information Security Oversight Office, the Director of the Office of Management and Budget, and the heads of affected agencies, the Secretary of Homeland Security shall serve as the Executive Agent for the Program. This order does not displace any authorities provided by law or Executive Order and the Executive Agent shall, to the extent practicable, make use of existing structures and authorities to preclude duplication and to ensure efficiency.

Sec. 3. SLTPS Policy Advisory Committee.

(a) There is established an SLTPS Policy Advisory Committee (Committee) to discuss Program-related policy issues in dispute in order to facilitate their resolution and to otherwise recommend changes to policies and procedures that are designed to remove undue impediments to the sharing of information under the Program. The Director of the Information Security Oversight Office shall serve as Chair of the Committee. An official designated by the Secretary of Homeland Security and a representative of SLTPS entities shall serve as Vice Chairs of the Committee. Members of the Committee shall include designees of the heads of the Departments of State, Defense, Justice, Transportation, and Energy, the Nuclear Regulatory Commission, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Federal Bureau of Investigation. Members shall also include employees of other agencies and representatives of SLTPS entities, as nominated by any Committee member and approved by the Chair.

(b) Members of the Committee shall serve without compensation for their work on the Committee, except that any representatives of SLTPS entities may be allowed travel expenses, including per diem in lieu of subsistence, as authorized

(c) The Information Security Oversight Office shall provide staff support to the Committee.

(d) Insofar as the Federal Advisory Committee Act, as amended (5 App. U.S.C.) (the “Act”) may apply to this order, any functions of the President under that Act, except that of reporting to the Congress, which are applicable to the Committee, shall be performed by the Administrator of General Services in accordance with guidelines and procedures established by the General Services Administration.

**Sec. 4. Operations and Oversight.**

(a) The Executive Agent for the Program shall perform the following responsibilities:

1. overall program management and oversight;

2. accreditation, periodic inspection, and monitoring of all facilities owned or operated by SLT entities that have access to classified information, except when another agency has entered into an agreement with the Department of Homeland Security to perform some or all of these functions;

3. processing of security clearance applications by SLTPS personnel, when requested by a sponsoring agency, on a reimbursable basis unless otherwise determined by the Department of Homeland Security and the sponsoring agency;

4. documenting and tracking the final status of security clearances for all SLTPS personnel in consultation with the Office of Personnel Management, the Department of Defense, and the Office of the Director of National Intelligence;

5. developing and maintaining a security profile of SLT facilities that have access to classified information; and

6. developing training, in consultation with the Committee, for all SLTPS personnel who have been determined eligible for access to classified information, which shall cover the proper safeguarding of classified information and sanctions for unauthorized disclosure of classified information.

(b) The Secretary of Defense, or the cognizant security agency under Executive Order 12829, as amended, shall provide program management, oversight, inspection, accreditation, and monitoring of all private sector facilities that have access to classified information.
(c) The Director of National Intelligence may inspect and monitor SLTPS programs and facilities that involve access to information regarding intelligence sources, methods, and activities.

(d) Heads of agencies that sponsor SLTPS personnel and facilities for access to and storage of classified information under section 1.3(a) of this order shall:

(1) ensure on a periodic basis that there is a demonstrated, foreseeable need for such access; and

(2) provide the Secretary of Homeland Security with information, as requested by the Secretary, about SLTPS personnel sponsored for security clearances and SLT facilities approved for use of classified information prior to and after the date of this order, except when the disclosure of the association of a specific individual with an intelligence or law enforcement agency must be protected in the interest of national security, as determined by the intelligence or law enforcement agency.

Sec. 5. Definitions.

For purposes of this order:

(a) “Access” means the ability or opportunity to gain knowledge of classified information.

(b) “Agency” means any “Executive agency” as defined in 5 U.S.C. 105; any military department as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into possession of classified information.

(c) “Classified National Security Information” or “classified information” means information that has been determined pursuant to Executive Order 13526, or any predecessor or successor order, to require protection against unauthorized disclosure, and is marked to indicate its classified status when in documentary form.

(d) “Information” means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(e) “Intelligence activities” means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(f) “Local” entities refers to “(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of
governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; and (B) a rural community, unincorporated town or village, or other public entity” as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101(11)).

(g) “Private sector” means persons outside government who are critically involved in ensuring that public and private preparedness and response efforts are integrated as part of the Nation’s Critical Infrastructure or Key Resources (CIKR), including:

(1) corporate owners and operators determined by the Secretary of Homeland Security to be part of the CIKR;

(2) subject matter experts selected to assist the Federal or State CIKR;

(3) personnel serving in specific leadership positions of CIKR coordination, operations, and oversight;

(4) employees of corporate entities relating to the protection of CIKR; or

(5) other persons not otherwise eligible for the granting of a personnel security clearance pursuant to Executive Order 12829, as amended, who are determined by the Secretary of Homeland Security to require a personnel security clearance.

(h) “Restricted portal” means a protected community of interest or similar area housed within an information system and to which access is controlled by a host agency different from the agency that controls the information system.

(i) “Sponsoring Agency” means an agency that recommends access to or possession of classified information by SLTPS personnel.

(j) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States, as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101(15)).

(k) “State, local, and tribal personnel” means any of the following persons:

(1) Governors, mayors, tribal leaders, and other elected or appointed officials of a State, local government, or tribe;

(2) State, local, and tribal law enforcement personnel and firefighters;
(3) public health, radiological health, and medical professionals of a State, local government, or tribe; and

(4) regional, State, local, and tribal emergency management agency personnel, including State Adjutants General and other appropriate public safety personnel and those personnel providing support to a Federal CIKR mission.

(l) “Tribe” means any Indian or Alaska Native tribe, band, nation, pueblo, village, or community that the Secretary of the Interior acknowledges to exist as an Indian tribe as defined in the Federally Recognized [Indian] Tribe List Act of 1994 (25 U.S.C. 479a(2)).

(m) “United States” when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States and any waters within the territorial jurisdiction of the United States.

Sec. 6. General Provisions.

(a) This order does not change the requirements of Executive Orders 13526, 12968, 13467, or 12829, as amended, and their successor orders and directives.

(b) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.); the Secretary of Defense under Executive Order 12829, as amended; the Director of the Information Security Oversight Office under Executive Order 13526 and Executive Order 12829, as amended; the Attorney General under title 18, United States Code, and the Foreign Intelligence Surveillance Act [of 1978] (50 U.S.C. 1801 et seq.); the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; or the Director of National Intelligence under the National Security Act of 1947, as amended, Executive Order 12333, as amended, Executive Order 12968, as amended, Executive Order 13467, and Executive Order 13526.

(c) Nothing in this order shall limit the authority of an agency head, or the agency head's designee, to authorize in an emergency and when necessary to respond to an imminent threat to life or in defense of the homeland, in accordance with section 4.2(b) of Executive Order 13526, the disclosure of classified information to an individual or individuals who are otherwise not eligible for access in accordance with the provisions of Executive Order 12968.
(d) Consistent with section 892(a)(4) of the Homeland Security Act of 2002 (6 U.S.C. 482(a)(4)), nothing in this order shall be interpreted as changing the requirements and authorities to protect sources and methods.

(e) Nothing in this order shall supersede measures established under the authority of law or Executive Order to protect the security and integrity of specific activities and associations that are in direct support of intelligence operations.

(f) Pursuant to section 892(e) of the Homeland Security Act of 2002 (6 U.S.C. 482(e)), all information provided to an SLTPS entity from an agency shall remain under the control of the Federal Government. Any State or local law authorizing or requiring disclosure shall not apply to such information.

(g) Nothing in this order limits the protection afforded any classified information by other provisions of law. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(h) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(i) This order shall be implemented subject to the availability of appropriations and consistent with procedures approved by the Attorney General pursuant to Executive Order 12333, as amended.

Sec. 7. Effective Date.

This order is effective 180 days from the date of this order with the exception of section 3, which is effective immediately.

Barack Obama.
Executive Order 13556: Controlled Unclassified Information (Nov. 4, 2010)

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose.
This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.
At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.
To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Section 2. Controlled Unclassified Information (CUI).
(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.
(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.
(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Section 3. Review of Current Designations.
(a) Each agency head shall, within 180 days of the date of this order:
(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.


(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.
(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Section 5. Implementation.

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.
(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.
(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.


(a) This order shall be implemented in a manner consistent with:
(1) applicable law, including protections of confidentiality and privacy rights;
(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and
(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.
(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.
(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.
(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the
United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled “Designation and Sharing of Controlled Unclassified Information (CUI)” is hereby rescinded.

BARACK OBAMA
The White House,
November 4, 2010.
Executive Order 13587. Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

Ex. Ord. No. 13587, Oct. 7, 2011, 76 F.R. 63811, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. Policy.

Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;
(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;
(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager—Information Sharing Environment (PM–ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD–1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Classified Information Sharing and Safeguarding Office.

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM–ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an
effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks.

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the “Executive Agent”), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD–42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent’s responsibilities, in addition to those specified by NSD–42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as redesignated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent’s timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.
Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;
(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. General Provisions.

(a) For the purposes of this order, the word “agencies” shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.


(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM–ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD–42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD–42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.
(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Barack Obama.
Implementation of the Executive Order, “Classified National Security Information”

Memorandum of President of the United States, Dec. 29, 2009, 75 F.R. 733, provided:

Memorandum for the Heads of Executive Departments and Agencies

Today I have signed an executive order [Ex. Ord. No. 13526, set out above] entitled, “Classified National Security Information” (the “order”), which substantially advances my goals for reforming the security classification and declassification processes. I expect that the order will produce measurable progress towards greater openness and transparency in the Government's classification and declassification programs while protecting the Government's legitimate interests, and I will closely monitor the results. I also look forward to reviewing recommendations from the study that the National Security Advisor will undertake in cooperation with the Public Interest Declassification Board to design a more fundamental transformation of the security classification system. To further assist in fulfilling the goal of measurable progress toward greater openness and transparency, I hereby direct the following actions.

1. Initial Implementation Efforts.

Successful implementation of the order requires personal commitment from the heads of departments and agencies, as well as their senior officials. It also requires effective security education and training programs, self-inspection programs, and measures designed to hold personnel accountable.

In accordance with section 5.4 of the order, the head of each department and agency that creates or handles classified information shall provide the Director of the Information Security Oversight Office (ISOO) a copy of the department or agency regulations implementing the requirements of the order. Such regulations shall be issued in final form within 180 days of ISOO's publication of its implementing directive for the order. The Director of ISOO shall consider agency actions to implement the requirements of section 5.4 of the order as a key element in planning oversight of agencies. Each senior agency official designated under section 5.4(d) of the order shall provide ISOO with updates concerning agency plans and other actions to implement the requirements of the order. The Director of ISOO shall publish a periodic status report on agency implementation.
2. Declassification of Records of Permanent Historical Value.

Under the direction of the National Declassification Center (NDC), and utilizing recommendations of an ongoing Business Process Review in support of the NDC, referrals and quality assurance problems within a backlog of more than 400 million pages of accessioned Federal records previously subject to automatic declassification shall be addressed in a manner that will permit public access to all declassified records from this backlog no later than December 31, 2013. In order to promote the efficient and effective utilization of finite resources available for declassification, further referrals of these records are not required except for those containing information that would clearly and demonstrably reveal: (a) the identity of a confidential human source or a human intelligence source; or (b) key design concepts of weapons of mass destruction.

The Secretaries of State, Defense, and Energy, and the Director of National Intelligence shall provide the Archivist of the United States with sufficient guidance to complete this task. The Archivist shall make public a report on the status of the backlog every 6 months.

3. Delegation of Original Classification Authority.

Delegations of original classification authority shall be limited to the minimum necessary to implement the order and only those individuals or positions with a demonstrable and continuing need to exercise such authority shall be delegated original classification authority.

Accordingly, heads of departments and agencies with original classification authority shall commence a review to ensure that all delegations of original classification authority are so limited and otherwise in accordance with section 1.3(c) of the order. Each department and agency shall submit a report on the results of this review to the Director of ISOO within 120 days of the date of this memorandum.


Striking the critical balance between openness and secrecy is a difficult but necessary part of our democratic form of government. Striking this balance becomes more difficult as the volume and complexity of the information increases. Improving the capability of departments and agencies to identify still-sensitive information and to make declassified information available to the public are integral parts of the classification system.
Therefore, I am directing that the Secretary of Defense and the Director of National Intelligence each support research to assist the NDC in addressing the cross-agency challenges associated with declassification.

5. Publication.

The Archivist of the United States is authorized and directed to publish this memorandum in the Federal Register.

Barack Obama.
Original Classification Authority

Order of President of the United States, dated Dec. 29, 2009, 75 F.R. 735, provided:

Pursuant to the provisions of section 1.3 of the Executive Order issued today [Ex. Ord. No. 13526, set out above], entitled “Classified National Security Information” (Executive Order), I hereby designate the following officials to classify information originally as “Top Secret” or “Secret”:

**TOP SECRET**

*Executive Office of the President:*

The Assistant to the President and Chief of Staff

The Assistant to the President for National Security Affairs (National Security Advisor)

The Assistant to the President for Homeland Security and Counterterrorism

The Director of National Drug Control Policy

The Director, Office of Science and Technology Policy

The Chair or Co-Chairs, President’s Intelligence Advisory Board

*Departments and Agencies:*

The Secretary of State

The Secretary of the Treasury

The Secretary of Defense

The Attorney General

The Secretary of Energy

The Secretary of Homeland Security

The Director of National Intelligence

The Secretary of the Army
The Secretary of the Navy
The Secretary of the Air Force
The Chairman, Nuclear Regulatory Commission
The Director of the Central Intelligence Agency
The Administrator of the National Aeronautics and Space Administration
The Director, Information Security Oversight Office

SECRET

Executive Office of the President:

The United States Trade Representative

Departments and Agencies:

The Secretary of Agriculture
The Secretary of Commerce
The Secretary of Health and Human Services
The Secretary of Transportation
The Administrator of the United States Agency for International Development
The Administrator of the Environmental Protection Agency

Any delegation of this authority shall be in accordance with section 1.3(c) of the Executive Order, except that the Director of the Information Security Oversight Office, the Secretary of Agriculture, and the Administrator of the Environmental Protection Agency may not delegate the authority granted in this order. If an agency head without original classification authority under this order, or otherwise delegated in accordance with section 1.3(c) of the Executive Order, has an exceptional need to classify information originated by their agency, the matter shall be referred to the agency head with appropriate subject matter interest and classification authority in accordance with section 1.3(e) of the Executive Order. If the agency with appropriate subject matter interest and classification authority cannot readily be determined, the matter shall be referred to the Director of the Information Security Oversight Office.
Presidential designations ordered prior to the issuance of the Executive Order are revoked as of the date of this order. However, delegations of authority to classify information originally that were made in accordance with the provisions of section 1.4 of Executive Order 12958 of April 17, 1995, as amended, by officials designated under this order shall continue in effect, provided that the authority of such officials is delegable under this order.

This order shall be published in the Federal Register.

Barack Obama.
LEGISLATIVE AGENCY RULES

Administrative Regulations Relevant to U.S. Intelligence Law
CFR TITLE 28—JUDICIAL ADMINISTRATION

28 CFR PART 5—ADMINISTRATION AND ENFORCEMENT OF FOREIGN AGENTS REGISTRATION ACT OF 1938, AS AMENDED

- 28 CFR Section 5.1: Administration and enforcement of the Act.
- 28 CFR Section 5.2: Inquiries concerning application of the Act.
- 28 CFR Section 5.3: Filing of a registration statement.
- 28 CFR Section 5.4: Computation of time.
- 28 CFR Section 5.5: Registration fees.
- 28 CFR Section 5.100: Definition of terms.
- 28 CFR Section 5.200: Registration.
- 28 CFR Section 5.201: Exhibits.
- 28 CFR Section 5.203: Supplemental statement.
- 28 CFR Section 5.204: Amendments.
- 28 CFR Section 5.205: Termination of registration.
- 28 CFR Section 5.206: Language and wording of registration statement.
- 28 CFR Section 5.207: Incorporation by reference.
- 28 CFR Section 5.209: Information relating to employees.
- 28 CFR Section 5.210: Amount of detail required in information relating to registrant’s activities and expenditures.
- 28 CFR Section 5.211: Sixty-day period to be covered in initial statement.
- 28 CFR Section 5.300: Burden of establishing availability of exemption.
- 28 CFR Section 5.301: Exemption under section 3(a) of the Act.
- 28 CFR Section 5.302: Exemptions under sections 3(b) and (c) of the Act.
- 28 CFR Section 5.303: Exemption available to persons accredited to international organizations.
- 28 CFR Section 5.304: Exemptions under sections 3(d) and (e) of the Act.
- 28 CFR Section 5.305: Exemption under section 3(f) of the Act.
- 28 CFR Section 5.306: Exemption under section 3(g) of the Act.
- 28 CFR Section 5.307: Exemption under 3(h) of the Act.
- 28 CFR Section 5.400: Filing of informational materials.
- 28 CFR Section 5.500: Maintenance of books and records.
- 28 CFR Section 5.501: Inspection of books and records.
- 28 CFR Section 5.600: Public examination of records.
- 28 CFR Section 5.601: Copies of records and information available.
- 28 CFR Section 5.800: Ten-day filing requirement.
- 28 CFR Section 5.801: Activity beyond 10-day period.

Authority:

Source: Order No. 376-67, 32 FR 6362, Apr. 22, 1967, unless otherwise noted.

28 CFR Section 5.1: Administration and enforcement of the Act.

(a) The administration and enforcement of the Foreign Agents Registration Act of 1938, as amended (22 U.S.C. 611-621) (Act), subject to the general supervision and direction of the Attorney General, is assigned to, and conducted, handled, and supervised by, the Assistant Attorney General for National Security.

(b) The Assistant Attorney General for National Security is authorized to prescribe such forms, in addition to or in lieu of those specified in the regulations in this part, as may be necessary to carry out the purposes of this part.

(c) Copies of the Act, and of the rules, regulations, and forms prescribed pursuant to the Act, and information concerning the foregoing may be obtained upon request without charge from the National Security Division, Department of Justice, Washington, DC 20530.

Official Citation: [Order No. 2865-2007, 72 FR 10068, Mar. 7, 2007]

28 CFR Section 5.2: Inquiries concerning application of the Act.

(a) General.
Any present or prospective agent of a foreign principal, or the agent's attorney, may request from the Assistant Attorney General for National Security a statement of the present enforcement intentions of the Department of Justice under the Act with respect to any presently contemplated activity, course of conduct, expenditure, receipt of money or thing of value, or transaction, and specifically with respect to whether the same requires registration and disclosure pursuant to the Act, or is excluded from coverage or exempted from registration and disclosure under any provision of the Act.

(b) Anonymous, hypothetical, non-party and ex post facto review requests excluded.
The entire transaction which is the subject of the review request must be an actual, as opposed to hypothetical, transaction and involve disclosed, as opposed to anonymous, agents and principals. Review requests must be submitted by a party to the transaction or the party’s attorney, and have no application to a party
that does not join in the request. A review request may not involve only past conduct.

(c) Fee. All requests for statements of the Department's present enforcement intentions must be accompanied by a non-refundable filing fee submitted in accordance with § 5.5.

(d) Address. A review request must be submitted in writing to the Assistant Attorney General for National Security, Department of Justice, Washington, DC 20530.

(e) Contents. A review request shall be specific and contain in detail all relevant and material information bearing on the actual activity, course of conduct, expenditure, receipt of money or thing of value, or transaction for which review is requested. There is no prescribed format for the request, but each request must include:

(1) The identity(ies) of the agent(s) and foreign principal(s) involved;

(2) The nature of the agent's activities for or in the interest of the foreign principal;

(3) A copy of the existing or proposed written contract with the foreign principal or a full description of the terms and conditions of each existing or proposed oral agreement; and

(4) The applicable statutory or regulatory basis for the exemption or exclusion claimed.

(f) Certification. If the requesting party is an individual, the review request must be signed by the prospective or current agent, or, if the requesting party is not an individual, the review request must be signed on behalf of each requesting party by an officer, a director, a person performing the functions of an officer or a director of, or an attorney for, the requesting party. Each such person signing the review request must certify that the review request contains a true, correct and complete disclosure with respect to the proposed conduct.

(g) Additional information. Each party shall provide any additional information or documents the National Security Division may thereafter request in order to review a matter. Any information furnished orally shall be confirmed promptly in writing, signed by the same person who signed the initial review request and certified to be a true, correct and complete disclosure of the requested information.
(h) Outcomes.
After submission of a review request, the National Security Division, in its discretion, may state its present enforcement intention under the Act with respect to the proposed conduct; may decline to state its present enforcement intention; or, if circumstances warrant, may take such other position or initiate such other action as it considers appropriate. Any requesting party or parties may withdraw a review request at any time. The National Security Division remains free, however, to submit such comments to the requesting party or parties as it deems appropriate. Failure to take action after receipt of a review request, documents or information, whether submitted pursuant to this procedure or otherwise, shall not in any way limit or stop the National Security Division from taking any action at such time thereafter as it deems appropriate. The National Security Division reserves the right to retain any review request, document or information submitted to it under this procedure or otherwise and to use any such request, document or information for any governmental purpose.

(i) Time for response.
The National Security Division shall respond to any review request within 30 days after receipt of the review request and of any requested additional information and documents.

(j) Written decisions only.
The requesting party or parties may rely only upon a written Foreign Agents Registration Act review letter signed by the Assistant Attorney General for National Security or his delegate.

(k) Effect of review letter.
Each review letter can be relied upon by the requesting party or parties to the extent the disclosure was accurate and complete and to the extent the disclosure continues accurately and completely to reflect circumstances after the date of issuance of the review letter.

(l) Compliance.
Neither the submission of a review request, nor its pendency, shall in any way alter the responsibility of the party or parties to comply with the Act.

(m) Confidentiality.
Any written material submitted pursuant to a request made under this section shall be treated as confidential and shall be exempt from disclosure.

Official Citation:
28 CFR Section 5.3: Filing of a registration statement.

All statements, exhibits, amendments, and other documents and papers required to be filed under the Act or under this part shall be submitted in triplicate to the Registration Unit. An original document and two duplicates meeting the requirements of Rule 1001(4), Federal Rules of Evidence (28 U.S.C. Appendix), shall be deemed to meet this requirement. Filing of such documents may be made in person or by mail, and they shall be deemed to be filed upon their receipt by the Registration Unit.

Official Citation:

28 CFR Section 5.4: Computation of time.

Sundays and holidays shall be counted in computing any period of time prescribed in the Act or in the rules and regulations in this part.

28 CFR Section 5.5: Registration fees.

(a) A registrant shall pay a registration fee with each initial registration statement filed under § 5.200 and each supplemental registration statement under § 5.203 at the time such registration statement is filed. The registration fee may be paid by cash or by check or money order made payable to “FARA Registration Unit”. The Registration Unit, in its discretion, may require that the fee be paid by a certified or cashier’s check or by a United States Postal money order.

(b) Payment of fees shall accompany any order for copies or request for information, and all applicable fees shall be collected before copies or information will be made available. Payment may be made by cash or by check or money order made payable to “FARA Registration Unit”. The Registration Unit, in its discretion, may require that the fee be paid by a certified or cashier’s check or by a United States Postal money order.

(c) Registration fees shall be waived in whole or in part, as appropriate, in the case of any individual person required to register under the Act who has demonstrated to the satisfaction of the Registration Unit that he or she is financially unable to pay the fees in their entirety. An individual seeking to avail himself or herself of this provision shall file with the registration statement a declaration made in compliance with section 1746 of title 28, United States Code,

(d) The fees shall be as follows:

(1) For initial registration statements (including an exhibit A for one foreign principal) under § 5.200: $305.00;

(2) For supplemental registration statements under § 5.203: $305.00 per foreign principal;

(3) For exhibit A under § 5.201(a)(1): $305.00 per foreign principal not currently reported under § 5.200 or § 5.203;

(4) For exhibit B under § 5.201(a)(2): no fee;

(5) For exhibits C and D (no forms) under § 5.201: no fee;

(6) For short-form registration statements under § 5.202: no fee;

(7) For amendments under § 5.204; no fee;

(8) For statements of present enforcement intentions under § 5.2: $96.00 per review request;

(9) For each quarter hour of search time under § 5.601: $4.00;

(10) For copies of registration statements and supplements, amendments, exhibits thereto, dissemination reports, informational materials, and copies of political propaganda and other materials contained in the public files, under § 5.601: fifty cents ($.50) per copy of each page of the material requested;

(11) For copies of registration statements and supplements, amendments, exhibits thereto, dissemination reports, informational materials, and copies of political propaganda and other materials contained in the public files, produced by computer, such as tapes or printouts, under § 5.601: actual direct cost of producing the copy, including the apportionable salary costs; and

(12) For computer searches of records through the use of existing programming: Direct actual costs, including the cost of operating a central processing unit for that portion of operating time that is directly attributable to searching for records responsive to a request and the salary costs apportionable to the search.
(e) The cost of delivery of any document by the Registration Unit by any means other than ordinary mail shall be charged to the requester at a rate sufficient to cover the expense to the Registration Unit.

(f) The Assistant Attorney General is hereby authorized to adjust the fees established by this section from time to time to reflect and recover the costs of the administration of the Registration Unit under the Act.

(g) Fees collected under this provision shall be available for the support of the Registration Unit.

(h) Notwithstanding § 5.3, no document required to be filed under the Act shall be deemed to have been filed unless it is accompanied by the applicable fee except as provided by paragraph (c) of this section.

**Official Citation:**
[Order No. 1757-93, 58 FR 37419, July 12, 1993, as amended by Order No. 2674-2003, 68 FR 33630, June 5, 2003]

28 CFR Section 5.100: Definition of terms.

(a) As used in this part:


(2) The term Attorney General means the Attorney General of the United States.

(3) The term Assistant Attorney General means the Assistant Attorney General for National Security, Department of Justice, Washington, DC 20530.

(4) The term Secretary of State means the Secretary of State of the United States.

(5) The term rules and regulations includes the regulations in this part and all other rules and regulations prescribed by the Attorney General pursuant to the Act and all registration forms and instructions thereon that may be prescribed by the regulations in this part or by the Assistant Attorney General for National Security.

(6) The term registrant means any person who has filed a registration statement with the Registration Unit, pursuant to section 2(a) of the Act and § 5.3.
(7) Unless otherwise specified, the term agent of a foreign principal means an agent of a foreign principal required to register under the Act.

(8) The term foreign principal includes a person any of whose activities are directed or indirectly supervised, directed, controlled, financed, or subsidized in whole or in major part by a foreign principal as that term is defined in section 1(b) of the Act.

(9) The term initial statement means the statement required to be filed with the Attorney General under section 2(a) of the Act.

(10) The term supplemental statement means the supplement required to be filed with the Attorney General under section 2(b) of the Act at intervals of 6 months following the filing of the initial statement.

(11) The term final statement means the statement required to be filed with the Attorney General following the termination of the registrant's obligation to register.

(12) The term short form registration statement means the registration statement required to be filed by certain partners, officers, directors, associates, employees, and agents of a registrant.

(b) As used in the Act, the term control or any of its variants shall be deemed to include the possession or the exercise of the power, directly or indirectly, to determine the policies or the activities of a person, whether through the ownership of voting rights, by contract, or otherwise.

(c) The term agency as used in sections 1(c), 1(o), 3(g), and 4(e) of the Act shall be deemed to refer to every unit in the executive and legislative branches of the Government of the United States, including committees of both Houses of Congress.

(d) The term official as used in sections 1(c), 1(o), 3(g), and 4(e) of the Act shall be deemed to include Members and officers of both Houses of Congress as well as officials in the executive branch of the Government of the United States.

(e) The terms formulating, adopting, or changing, as used in section 1(o) of the Act, shall be deemed to include any activity which seeks to maintain any existing domestic or foreign policy of the United States. They do not include making a routine inquiry of a Government official or employee concerning a current policy or seeking administrative action in a matter where such policy is not in question.

(f) The term domestic or foreign policies of the United States, as used in sections 1(o) and (p) of the Act, shall be deemed to relate to existing and proposed
legislation, or legislative action generally; treaties; executive agreements, proclamations, and orders; decisions relating to or affecting departmental or agency policy, and the like.

**Official Citation:**

---

**28 CFR Section 5.200: Registration.**

(a) Registration under the Act is accomplished by the filing of an initial statement together with all the exhibits required by § 5.201 and the filing of a supplemental statement at intervals of 6 months for the duration of the principal-agent relationship requiring registration.

(b) The initial statement shall be filed on a form provided by the Registration Unit.

Authority: (28 U.S.C. 509 and 510; 5 U.S.C. 301)

**Official Citation:**

---

**28 CFR Section 5.201: Exhibits.**

(a) The following described exhibits are required to be filed for each foreign principal of the registrant:

   (1) Exhibit A.
   This exhibit, which shall be filed on a form provided by the Registration Unit, shall set forth the information required to be disclosed concerning each foreign principal.

   (2) Exhibit B.
   This exhibit, which shall be filed on a form provided by the Registration Unit, shall set forth the agreement or understanding between the registrant and each of his foreign principals as well as the nature and method of performance of such agreement or understanding and the existing or proposed activities engaged in or to be engaged in, including political activities, by the registrant for the foreign principal.
(b) Any change in the information furnished in exhibit A or B shall be reported to the Registration Unit within 10 days of such change. The filing of a new exhibit may then be required by the Assistant Attorney General.

(c) Whenever the registrant is an association, corporation, organization, or any other combination of individuals, the following documents shall be filed as exhibit C:

1. A copy of the registrant's charter, articles of incorporation or association, or constitution, and a copy of its bylaws, and amendments thereto;

2. A copy of every other instrument or document, and a statement of the terms and conditions of every oral agreement, relating to the organization, powers and purposes of the registrant.

(d) The requirement to file any of the documents described in paragraphs (c)(1) and (2) of this section may be wholly or partially waived upon written application by the registrant to the Assistant Attorney General setting forth fully the reasons why such waiver should be granted.

(e) Whenever a registrant, within the United States, receives or collects contributions, loans, money, or other things of value, as part of a fund-raising campaign, for or in the interests of his foreign principal, he shall file as exhibit D a statement so captioned setting forth the amount of money or the value of the thing received or collected, the names and addresses of the persons from whom such money or thing of value was received or collected, and the amount of money or a description of the thing of value transmitted to the foreign principal as well as the manner and time of such transmission.

 Authority: (28 U.S.C. 509 and 510; 5 U.S.C. 301)

Official Citation:

28 CFR Section 5.202: Short form registration statement.

(a) Except as provided in paragraphs (b), (c), and (d) of this section, each partner, officer, director, associate, employee, and agent of a registrant is required to file a registration statement under the Act. Unless the Assistant Attorney General specifically directs otherwise, this obligation may be satisfied by the filing of a short form registration statement.
(b) A partner, officer, director, associate, employee, or agent of a registrant who does not engage directly in registrable activity in furtherance of the interests of the foreign principal is not required to file a short form registration statement.

(c) An employee or agent of a registrant whose services in furtherance of the interests of the foreign principal are rendered in a clerical, secretarial, or in a related or similar capacity, is not required to file a short form registration statement.

(d) Whenever the agent of a registrant is a partnership, association, corporation, or other combination of individuals, and such agent is not within the exemption of paragraph (b) of this section, only those partners, officers, directors, associates, and employees who engage directly in activity in furtherance of the interests of the registrant's foreign principal are required to file a short form registration statement.

(e) The short form registration statement shall be filed on Form OBD-66. Any change affecting the information furnished with respect to the nature of the services rendered by the person filing the statement, or the compensation he receives, shall require the filing of a new short form registration statement within 10 days after the occurrence of such change. There is no requirement to file exhibits or supplemental statements to a short form registration statement.

Authority: (28 U.S.C. 509 and 510; 5 U.S.C. 301)

Official Citation:

28 CFR Section 5.203: Supplemental statement.

(a) Supplemental statements shall be filed on a form provided by the Registration Unit.

(b) The obligation to file a supplemental statement at 6-month intervals during the agency relationship shall continue even though the registrant has not engaged during the period in any activity in the interests of his foreign principal.

(c) The time within which to file a supplemental statement may be extended for sufficient cause shown in a written application to the Assistant Attorney General.

Authority: (28 U.S.C. 509 and 510; 5 U.S.C. 301)
28 CFR Section 5.204: Amendments.

(a) An initial, supplemental, or final statement which is deemed deficient by the Assistant Attorney General must be amended upon his request. Such amendment shall be filed upon a form provided by the Registration Unit and shall identify the item of the statement to be amended.

(b) A change in the information furnished in an initial or supplemental statement under clauses (3), (4), (6), and (9) of section 2(a) of the Act shall be by amendment, unless the notice which is required to be given of such change under section 2(b) is deemed sufficient by the Assistant Attorney General.

Authority: (28 U.S.C. 509 and 510; 5 U.S.C. 301)

28 CFR Section 5.205: Termination of registration.

(a) A registrant shall, within 30 days after the termination of his obligation to register, file a final statement on the supplemental statement form with the Registration Unit for the final period of the agency relationship not covered by any previous statement.

(b) Registration under the Act shall be terminated upon the filing of a final statement, if the registrant has fully discharged all his obligations under the Act.

(c) A registrant whose activities on behalf of each of his foreign principals become confined to those for which an exemption under section 3 of the Act is available may file a final statement notwithstanding the continuance of the agency relationship with the foreign principals.

(d) Registration under the Act may be terminated upon a finding that the registrant is unable to file the appropriate forms to terminate the registration as a result of the death, disability, or dissolution of the registrant or where the requirements of the Act cannot be fulfilled by a continuation of the registration.
Authority: (28 U.S.C. 509 and 510; 5 U.S.C. 301)

Official Citation:

28 CFR Section 5.206: Language and wording of registration statement.

(a) Except as provided in the next sentence, each statement, amendment, exhibit, or notice required to be filed under the Act shall be submitted in the English language. An exhibit may be filed even though it is in a foreign language if it is accompanied by an English translation certified under oath by the translator before a notary public, or other person authorized by law to administer oaths for general purposes, as a true and accurate translation.

(b) A statement, amendment, exhibit, or notice required to be filed under the Act should be typewritten, but will be accepted for filing if it is written legibly in ink, or if it is filed in an electronic format acceptable to the Registration Unit.

(c) Copies of any document made by any of the duplicating processes may be filed pursuant to the Act if they are clear and legible.

(d) A response shall be made to every item on each pertinent form, unless a registrant is specifically instructed otherwise in the form. Whenever the item is inapplicable or the appropriate response to an item is “none,” an express statement to that effect shall be made.

Official Citation:

28 CFR Section 5.207: Incorporation by reference.

(a) Each initial, supplemental, and final statement shall be complete in and of itself. Incorporation of information by reference to statements previously filed is not permissible.
(b) Whenever insufficient space is provided for response to any item in a form, reference shall be made in such space to a full insert page or pages on which the item number and inquiry shall be restated and a complete answer given. Inserts and riders of less than full page size should not be used.

28 CFR Section 5.208: Disclosure of foreign principals.

A registrant who represents more than one foreign principal is required to list in the statements he files under the Act only those foreign principals for whom he is not entitled to claim exemption under section 3 of the Act.

28 CFR Section 5.209: Information relating to employees.

A registrant shall list in the statements he files under the Act only those employees whose duties require them to engage directly in activities in furtherance of the interests of the foreign principal.

28 CFR Section 5.210: Amount of detail required in information relating to registrant’s activities and expenditures.

A statement is “detailed” within the meaning of clauses 6 and 8 of section 2 (a) of the Act when it has that degree of specificity necessary to permit meaningful public evaluation of each of the significant steps taken by a registrant to achieve the purposes of the agency relation.

28 CFR Section 5.211: Sixty-day period to be covered in initial statement.

The 60-day period referred to in clauses 5, 7, and 8 of section 2(a) of the Act shall be measured from the time that a registrant has incurred an obligation to register and not from the time that he files his initial statement.

28 CFR Section 5.300: Burden of establishing availability of exemption.
The burden of establishing the availability of an exemption from registration under the Act shall rest upon the person for whose benefit the exemption is claimed.

28 CFR Section 5.301: Exemption under section 3(a) of the Act.

(a) A consular officer of a foreign government shall be considered duly accredited under section 3(a) of the Act whenever he has received formal recognition as such, whether provisionally or by exequatur, from the Secretary of State.

(b) The exemption provided by section 3(a) of the Act to a duly accredited diplomatic or consular officer is personal and does not include within its scope an office, bureau, or other entity.

28 CFR Section 5.302: Exemptions under sections 3(b) and (c) of the Act.

The exemptions provided by sections 3(b) and (c) of the Act shall not be available to any person described therein unless he has filed with the Secretary of State a fully executed Notification of Status with a Foreign Government (Form D.S. 394).

28 CFR Section 5.303: Exemption available to persons accredited to international organizations.

Persons designated by foreign governments as their representatives in or to an international organization, other than nationals of the United States, are exempt from registration under the Act in accordance with the provisions of the International Organizations Immunities Act, if they have been duly notified to and accepted by the Secretary of State as such representatives, officers, or employees, and if they engage exclusively in activities which are recognized as being within the scope of their official functions.

28 CFR Section 5.304: Exemptions under sections 3(d) and (e) of the Act.

(a) As used in section 3(d), the term trade or commerce shall include the exchange, transfer, purchase, or sale of commodities, services, or property of any kind.
(b) For the purpose of section 3(d) of the Act, activities of an agent of a foreign principal as defined in section 1(c) of the Act, in furtherance of the bona fide trade or commerce of such foreign principal, shall be considered “private,” even though the foreign principal is owned or controlled by a foreign government, so long as the activities do not directly promote the public or political interests of the foreign government.

(c) For the purpose of section 3(d)(2) of the Act, a person engaged in political activities on behalf of a foreign corporation, even if owned in whole or in part by a foreign government, will not be serving predominantly a foreign interest where the political activities are directly in furtherance of the bona fide commercial, industrial, or financial operations of the foreign corporation, so long as the political activities are not directed by a foreign government or foreign political party and the political activities do not directly promote the public or political interests of a foreign government or of a foreign political party.

(d) The exemption provided by section 3(e) of the Act shall not be available to any person described therein if he engages in political activities as defined in section 1(o) of the Act for or in the interests of his foreign principal.

Official Citation:

28 CFR Section 5.305: Exemption under section 3(f) of the Act.

The exemption provided by section 3(f) of the Act shall not be available unless the President has, by publication in the Federal Register, designated for the purpose of this section the country the defense of which he deems vital to the defense of the United States.

28 CFR Section 5.306: Exemption under section 3(g) of the Act.

For the purpose of section 3(g) of the Act—

(a) Attempts to influence or persuade agency personnel or officials other than in the course of judicial proceedings, criminal or civil law enforcement inquiries, investigations, or proceedings, or agency proceedings required by statute or regulation to be conducted on the record, shall include only such attempts to influence or persuade with reference to formulating, adopting, or changing the
domestic or foreign policies of the United States or with reference to the political or public interests, policies, or relations of a government of a foreign country or a foreign political party; and

(b) If an attorney engaged in legal representation of a foreign principal before an agency of the U.S. Government is not otherwise required to disclose the identity of his principal as a matter of established agency procedure, he must make such disclosure, in conformity with this section of the Act, to each of the agency’s personnel or officials before whom and at the time his legal representation is undertaken. The burden of establishing that the required disclosure was made shall fall upon the person claiming the exemption.

Official Citation:

28 CFR Section 5.307: Exemption under 3(h) of the Act.

For the purpose of section 3(h) of the Act, the burden of establishing that registration under the Lobbying Disclosure Act of 1995, 2 U.S.C. 1601 et seq. (LDA), has been made shall fall upon the person claiming the exemption. The Department of Justice will accept as prima facie evidence of registration a duly executed registration statement filed pursuant to the LDA. In no case where a foreign government or foreign political party is the principal beneficiary will the exemption under 3(h) be recognized.

Official Citation:
[Order No. 2674-2003, 68 FR 33631, June 5, 2003]

28 CFR Section 5.400: Filing of informational materials.

(a) The informational materials required to be filed with the Attorney General under section 4(a) of the Act shall be filed with the Registration Unit no later than 48 hours after the beginning of the transmittal of the informational materials.

(b) Whenever informational materials have been filed pursuant to section 4(a) of the Act, an agent of a foreign principal shall not be required, in the event of further dissemination of the same materials, to forward additional copies thereof to the Registration Unit.
(c) Unless specifically directed to do so by the Assistant Attorney General, a registrant is not required to file a copy of a motion picture which he disseminates on behalf of his foreign principal, so long as he files monthly reports on its dissemination. In each such case this registrant shall submit to the Registration Unit either a film strip showing the label required by section 4(b) of the Act or an affidavit certifying that the required label has been made a part of the film.

**Official Citation:**

**28 CFR Section 5.402: Labeling informational materials.**

(a) Within the meaning of this part, informational materials shall be deemed labeled whenever they have been marked or stamped conspicuously at their beginning with a statement setting forth such information as is required under section 4(b) of the Act.

(b) Informational materials which are required to be labeled under section 4(b) of the Act and which are in the form of prints shall be marked or stamped conspicuously at the beginning of such materials with a statement in the language or languages used therein, setting forth such information as is required under section 4(b) of the Act.

(c) Informational materials required to be labeled under section 4(b) of the Act but which are not in the form of prints shall be accompanied by a statement setting forth such information as is required under section 4(b) of the Act.

(d) Informational materials that are televised or broadcast, or which are caused to be televised or broadcast, by an agent of a foreign principal, shall be introduced by a statement which is reasonably adapted to convey to the viewers or listeners thereof such information as is required under section 4(b) of the Act.

(e) An agent of a foreign principal who transmits or causes to be transmitted in the U.S. mails or by any means or instrumentality of interstate or foreign commerce a still or motion picture film which contains informational materials shall insert at the beginning of such film a statement which is reasonably adapted to convey to the viewers thereof such information as is required under section 4(b) of the Act.
(f) For the purpose of section 4(e) of the Act, the statement that must preface or accompany informational materials or a request for information shall be in writing.

**Official Citation:**

28 CFR Section 5.500: Maintenance of books and records.

(a) A registrant shall keep and preserve in accordance with the provisions of section 5 of the Act the following books and records:

(1) All correspondence, memoranda, cables, telegrams, teletype messages, and other written communications to and from all foreign principals and all other persons, relating to the registrant's activities on behalf of, or in the interest of any of his foreign principals.

(2) All correspondence, memoranda, cables, telegrams, teletype messages, and other written communications to and from all persons, other than foreign principals, relating to the registrant's political activity, or relating to political activity on the part of any of the registrant's foreign principals.

(3) Original copies of all written contracts between the registrant and any of his foreign principals.

(4) Records containing the names and addresses of persons to whom informational materials have been transmitted.

(5) All bookkeeping and other financial records relating to the registrant's activities on behalf of any of his foreign principals, including canceled checks, bank statements, and records of income and disbursements, showing names and addresses of all persons who paid moneys to, or received moneys from, the registrant, the specific amounts so paid or received, and the date on which each item was paid or received.

(6) If the registrant is a corporation, partnership, association, or other combination of individuals, all minute books.

(7) Such books or records as will disclose the names and addresses of all employees and agents of the registrant, including persons no longer acting as such employees or agents.
(8) Such other books, records, and documents as are necessary properly to reflect the activities for which registration is required.

(b) The books and records listed in paragraph (a) of this section shall be kept and preserved in such manner as to render them readily accessible for inspection pursuant to section 5 of the Act.

(c) A registrant shall keep and preserve the books and records listed in paragraph (a) of this section for a period of 3 years following the termination of his registration under § 5.205.

(d) Upon good and sufficient cause shown in writing to the Assistant Attorney General, a registrant may be permitted to destroy books and records in support of the information furnished in an initial or supplemental statement which he filed 5 or more years prior to the date of his application to destroy.

Official Citation:

28 CFR Section 5.501: Inspection of books and records.

Officials of the National Security Division and the Federal Bureau of Investigation are authorized under section 5 of the Act to inspect the books and records listed in § 5.500(a).

Official Citation:

28 CFR Section 5.600: Public examination of records.

Registration statements, informational materials, Dissemination Reports, and copies of political propaganda filed under section 4(a) of the Act, shall be available for public examination at the Registration Unit on official business days, during the posted hours of operation.

Official Citation:
**28 CFR Section 5.601: Copies of records and information available.**

(a) Copies of registration statements and supplements, amendments, exhibits thereto, informational materials, dissemination reports, and copies of political propaganda and other materials contained in the public files, may be obtained from the Registration Unit upon payment of a fee as prescribed in § 5.5.

(b) Information as to the fee to be charged for copies of registration statements and supplements, amendments, exhibits thereto, informational materials, dissemination reports, and copies of political propaganda and other materials contained in the public files, or research into and information therefrom, and the time required for the preparation of such documents or information may be obtained upon request to the Registration Unit. Fee rates are established in § 5.5.

(c) The Registration Unit may, in its discretion, conduct computer searches of records through the use of existing programming upon written request. Information as to the fee for the conduct of such computer searches, and the time required to conduct such computer searches, may be obtained upon request to the Registration Unit. A written request for computer searches of records shall include a deposit in the amount specified by the Registration Unit, which shall be the Registration Unit's estimate of the actual fees. The Registration Unit is not required to alter or develop programming to conduct a search. Fee rates are established in § 5.5.

**Official Citation:**

**28 CFR Section 5.800: Ten-day filing requirement.**

The 10-day filing requirement provided by section 8(g) of the Act shall be deemed satisfied if the amendment to the registration statement is deposited in the U.S. mails no later than the 10th day of the period.

**28 CFR Section 5.801: Activity beyond 10-day period.**

A registrant who has within the 10-day period filed an amendment to his registration statement pursuant to a Notice of Deficiency given under section 8(g) of the Act may continue to act as an agent of a foreign principal beyond this period unless he receives a Notice of Noncompliance from the Registration Unit.
Official Citation:


Copies of the Report of the Attorney General to the Congress on the Administration of the Foreign Agents Registration Act of 1938, as amended, shall be sold to the public by the Registration Unit, as available, at a charge not less than the actual cost of production and distribution.

Official Citation:
[Order No. 1757-93, 58 FR 37420, July 12, 1993]
Registration Statement
- 28 CFR Section 10.1: Form of registration statement.
- 28 CFR Section 10.2: Language of registration statement.
- 28 CFR Section 10.3: Effect of acceptance of registration statement.
- 28 CFR Section 10.4: Date of filing.
- 28 CFR Section 10.5: Incorporation of papers previously filed.
- 28 CFR Section 10.6: Necessity for further registration.
- 28 CFR Section 10.7: Cessation of activity.

Supplemental Registration Statement
- 28 CFR Section 10.8: Information to be kept current.
- 28 CFR Section 10.9: Requirements for supplemental registration statement.

Inspection of Registration Statement
- 28 CFR Section 10.10: Public inspection.

Authority:

Cross References:
For regulations under the Foreign Agents Registration Act, see part 5 of this chapter.

For Organization Statement, Internal Security Section, see subpart K of part o of this chapter.

Source:
6 FR 369, Jan. 15, 1941, unless otherwise noted.
REGISTRATION STATEMENT

28 CFR Section 10.1: Form of registration statement.

Every organization required to submit a registration statement\(^1\) to the Attorney General for filing in compliance with the terms of section 2 of the act approved October 17, 1940, entitled, “An act to require the registration of certain organizations carrying on activities within the United States, and for other purposes” (Pub. L. 772, 80th Cong.; 18 U.S.C. 2386), and the rules and regulations issued pursuant thereto, shall submit such statement on such forms as are prescribed by the Attorney General. Every statement required to be filed with the Attorney General shall be subscribed under oath by all of the officers of the organization registering.

28 CFR Section 10.2: Language of registration statement.

Registration statements must be in English if possible. If in a foreign language they must be accompanied by an English translation certified under oath by the translator, before a notary public or other person authorized by law to administer oaths for general purposes as a true and adequate translation. The statements, with the exception of signature, must be typewritten if practicable but will be accepted if written legibly in ink.

28 CFR Section 10.3: Effect of acceptance of registration statement.

Acceptance by the Attorney General of a registration statement submitted for filing shall not necessarily signify a full compliance with the said act on the part of the registrant, and such acceptance shall not preclude the Attorney General from seeking such additional information as he deems necessary under the

---

\(^1\) Filed as a part of the original document. Copies may be obtained from the Department of Justice.
requirements of the said act, and shall not preclude prosecution as provided for in the said act for a false statement of a material fact, or the willful omission of a material fact required to be stated therein, or necessary to make the statements made not misleading.

28 CFR Section 10.4: Date of filing.

The date on which a registration statement properly executed is accepted by the Attorney General for filing shall be considered the date of the filing of such registration statement pursuant to the said act. All statements must be filed not later than thirty days after January 15, 1941.

28 CFR Section 10.5: Incorporation of papers previously filed.

Papers and documents already filed with the Attorney General pursuant to the said act and regulations issued pursuant thereto may be incorporated by reference in any registration statement subsequently submitted to the Attorney General for filing, provided such papers and documents are adequately identified in the registration statement in which they are incorporated by reference.

28 CFR Section 10.6: Necessity for further registration.

The filing of a registration statement with the Attorney General as required by the act shall not operate to remove the necessity for filing a registration statement with the Attorney General as required by the act of June 8, 1938, as amended, entitled “An act to require the registration of certain persons employed by agencies to disseminate propaganda in the United States and for other purposes” (52 Stat. 631, 56 Stat. 248; 22 U.S.C. 611), or for filing a notification statement with the Secretary of State as required by the act of June 15, 1917 (40 Stat. 226).

Official Citation:
[13 FR 8292, Dec. 24, 1948]

28 CFR Section 10.7: Cessation of activity.

The chief officer or other officer of the registrant organization must notify the Attorney General promptly upon the cessation of the activity of the organization,
its branches, chapters, or affiliates by virtue of which registration has been required pursuant to the act.

**Supplemental Registration Statement**

**28 CFR Section 10.8: Information to be kept current.**

A supplemental statement must be filed with the Attorney General within thirty days after the expiration of each period of six months succeeding the original filing of a registration statement. Each supplemental statement must contain information and documents as may be necessary to make information and documents previously filed accurate and current with respect to the preceding six months’ period.

**28 CFR Section 10.9: Requirements for supplemental registration statement.**

The rules and regulations in this part with respect to registration statements submitted to the Attorney General under section 2 of the said act shall apply with equal force and effect to supplemental registration statements required thereunder to be filed with the Attorney General.

**Inspection of Registration Statement**

**28 CFR Section 10.10: Public inspection.**

Registration statements filed with the Attorney General pursuant to the said act shall be available for public inspection in the Department of Justice, Washington, DC, from 10 a.m. to 4 p.m. on each official business day.

**Official Citation:**

[13 FR 8292, Dec. 24, 1948]
28 CFR PART 12—REGISTRATION OF CERTAIN PERSONS HAVING KNOWLEDGE OF FOREIGN ESPIONAGE, COUNTERESPIONAGE, OR SABOTAGE MATTERS UNDER THE ACT OF AUGUST 1, 1956

- 28 CFR Section 12.1: Definitions.
- 28 CFR Section 12.2: Administration of act.
- 28 CFR Section 12.3: Prior registration with the Foreign Agents Registration Unit.
- 28 CFR Section 12.4: Inquiries concerning application of act.
- 28 CFR Section 12.21: Time within which registration statement must be filed.
- 28 CFR Section 12.23: Deficient registration statement.
- 28 CFR Section 12.30: Burden of establishing availability of exemptions.
- 28 CFR Section 12.41: Photocopies.
- 28 CFR Section 12.70: Partial compliance not deemed compliance.

Authority:

Cross Reference:
For Organization Statement, Internal Security Section, see subpart K of part 0 of this chapter.

Source:
21 FR 5928, Aug. 8, 1956, unless otherwise noted.
28 CFR Section 12.1: Definitions.

As used in this part, unless the context otherwise requires:

(a) The term act means the act of August 1, 1956, Public Law 893, 84th Congress, 2d Session, requiring the registration of certain persons who have knowledge of, or have received instruction or assignment in the espionage, counterespionage, or sabotage service or tactics of a foreign government or foreign political party.

(b) The term Attorney General means the Attorney General of the United States.

(c) The term rules and regulations refers to all rules, regulations, registration forms, and instruction to forms made and prescribed by the Attorney General pursuant to the act.

(d) The term registration statement means the registration required to be filed with the Attorney General under section 2 of the act.

(e) The term registrant means the person by whom a registration statement is filed pursuant to the provisions of the act.

28 CFR Section 12.2: Administration of act.

The administration of the act is assigned to the National Security Division, Department of Justice. Communications with respect to the act shall be addressed to the National Security Division, Department of Justice, Washington, DC 20530. Copies of the act and the regulations contained in this part, including the forms mentioned therein, may be obtained upon request without charge.

Official Citation:

28 CFR Section 12.3: Prior registration with the Foreign Agents Registration Unit.

No person who has filed a registration statement under the terms of the Foreign Agents Registration Act of 1938, as amended by section 20(a) of the Internal Security Act of 1950, shall be required to file a registration statement under the act, unless otherwise determined by the Chief, Registration Unit.

Official Citation:
28 CFR Section 12.4: Inquiries concerning application of act.

Inquiries concerning the application of the act must be accompanied by a detailed statement of all facts necessary for a determination of the question submitted, including the identity of the person on whose behalf the inquiry is made, the facts which may bring such person within the registration provisions of the act, and the identity of the foreign government or foreign political party concerned.

28 CFR Section 12.20: Filing of registration statement.

Registration statements shall be filed in duplicate with the National Security Division, Department of Justice, Washington, DC 20530. Filing may be made in person or by mail, and shall be deemed to have taken place upon the receipt thereof by the Division.

Official Citation:

28 CFR Section 12.21: Time within which registration statement must be filed.

Every person who is or becomes subject to the registration provisions of the act after its effective date shall file a registration statement within fifteen days after the obligation to register arises.


The registration statement shall include the following, all of which shall be regarded as material for the purposes of the act:

(a) The registrant’s name, principal business address, and all other business addresses in the United States or elsewhere, and all residence addresses.

(b) The registrant’s citizenship status and how such status was acquired.
(c) A detailed statement setting forth the nature of the registrant’s knowledge of
the espionage, counterespionage, or sabotage service or tactics of a foreign
government or foreign political party, and the manner in which, place where, and
date when such knowledge was obtained.

(d) A detailed statement as to any instruction or training received by the
registrant in the espionage, counterespionage, or sabotage service or tactics of a
foreign government or foreign political party, including a description of the type
of instruction or training received, a description of any courses taken, the dates
when such courses commenced and when they ceased, and the name and official
title of the instructor or instructors under whose supervision the courses were
received as well as the name and location of schools and other institutions
attended, the dates of such attendance, and the names of the directors of the
schools and institutions attended.

(e) A detailed statement describing any assignment received in the espionage,
counterespionage, or sabotage service or tactics of a foreign government or
foreign political party, including the type of assignment, the date when each
assignment began, the date of completion of each assignment, name and title of
the person or persons under whose supervision the assignment was executed,
and a complete description of the nature of the assignment and the execution
thereof.

(f) A detailed statement of any relationship which may exist at the time of
registration, other than through employment, between the registrant and any
foreign government or foreign political party.

(g) Such other statements, information, or documents pertinent to the purposes
and objectives of the act as the Attorney General, having due regard for the
national security and the public interest, may require by this part or amendments
thereto.

28 CFR Section 12.23: Deficient registration statement.

A registration statement which is determined to be incomplete, inaccurate,
misleading, or false, by the Chief Registration Unit, may be returned by him to
the registrant as being unacceptable for filing under the terms of the act.

Official Citation:
[21 FR 5928, Aug. 8, 1956, as amended by Order No. 524-73, 38 FR 18235, July
9, 1973]

(a) Every person required to register under the act shall file a registration statement on Form GA-1, and such other forms as may from time to time be prescribed by the Attorney General.

(b) Matter contained in any part of the registration statement or other document may not be incorporated by reference as answer, or partial answer, to any other item in the registration statement required to be filed under the act.

(c) Except as specifically provided otherwise, if any item on the form is inapplicable, or the answer is “None,” an express statement to such effect shall be made.

(d) Every statement, amendment, and every duplicate thereof, shall be executed under oath and shall be sworn to before a notary public or other officer authorized to administer oaths.

(e) A registration statement or amendment thereof required to be filed shall, if possible, be typewritten, but will be regarded as in substantial compliance with this regulation if written legibly in black ink.

(f) Riders shall not be used. If the space on the registration statement or other form is insufficient for any answer, reference shall be made in the appropriate space to a full insert page or pages on which the item number and item shall be restated and the complete answer given.

28 CFR Section 12.25: Amended registration statement.

(a) An amended registration statement may be required by the Chief, Registration Unit, of any person subject to the registration provisions of the act whose original registration statement filed pursuant thereto is deemed to be incomplete, inaccurate, false, or misleading.

(b) Amendments shall conform in all respects to the regulations herein prescribed governing execution and filing of original registration statements.

(c) Amendments shall in every case make appropriate reference by number or otherwise to the items in original registration statements to which they relate.

(d) Amendments shall be deemed to have been filed upon the receipt thereof by the Registration Unit.
(e) Failure of the Chief, Registration Unit, to request any person described in section 2 of the act to file an amended registration statement shall not preclude prosecution of such person for a willfully false statement of a material fact, the willful omission of a material fact, or the willful omission of a material fact necessary to make the statements therein not misleading, in an original registration statement.

**Official Citation:**
[21 FR 5928, Aug. 8, 1956, as amended by Order No. 524-73, 38 FR 18235, July 9, 1973]

**28 CFR Section 12.30: Burden of establishing availability of exemptions.**

In all matters pertaining to exemptions, the burden of establishing the availability of the exemption shall rest with the person for whose benefit the exemption is claimed.

**28 CFR Section 12.40: Public examination.**

Registration statements shall be available for public examination at the offices of the Registration Unit, Department of Justice, Washington, DC, from 10 a.m. to 4 p.m. on each official business day, except to the extent that the Attorney General having due regard for national security and public interest may withdraw such statements from public examination.

**Official Citation:**
[Order No. 524-73, 38 FR 18235, July 9, 1973]

**28 CFR Section 12.41: Photocopies.**

(a) Photocopies of registration statements filed in accordance with section 2 of the act are available to the public upon payment of fifty cents per photocopy of each page, whether several copies of a single original page or one or more copies of several original pages are ordered.

(b) Estimates as to prices for photocopies and the time required for their preparation will be furnished upon request addressed to the Registration Unit, Internal Security Section, Criminal Division, Department of Justice, Washington, DC 20530.
(c) Payment shall accompany the order for photocopies and shall be made in cash, or by United States money order, or by certified bank check payable to the Treasurer of the United States. Postage stamps will not be accepted.

**Official Citation:**
[21 FR 5928, Aug. 8, 1956, as amended by Order No. 524-73, 38 FR 18235, July 9, 1973]

**28 CFR Section 12.70: Partial compliance not deemed compliance.**

The fact that a registration statement has been filed shall not necessarily be deemed a full compliance with the act on the part of the registrant; nor shall it preclude prosecution, as provided for in the act, for willful failure to file a registration statement, or for a willfully false statement of a material fact therein, or for the willful omission of a material fact required to be stated therein.
28 CFR PART 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

➤ Subpart A—Procedures for Disclosure of Records Under the Freedom of Information Act
  o 28 CFR Section 16.1: General provisions.
  o 28 CFR Section 16.2: Public reading rooms.
  o 28 CFR Section 16.3: Requirements for making requests.
  o 28 CFR Section 16.4: Responsibility for responding to requests.
  o 28 CFR Section 16.5: Timing of responses to requests.
  o 28 CFR Section 16.6: Responses to requests.
  o 28 CFR Section 16.7: Classified information.
  o 28 CFR Section 16.8: Business information.
  o 28 CFR Section 16.9: Appeals.
  o 28 CFR Section 16.10: Preservation of records.
  o 28 CFR Section 16.11: Fees.
  o 28 CFR Section 16.12: Other rights and services.

➤ Subpart B—Production or Disclosure in Federal and State Proceedings
  o 28 CFR Section 16.21: Purpose and scope.
  o 28 CFR Section 16.22: General prohibition of production or disclosure in Federal and State proceedings in which the United States is not a party.
  o 28 CFR Section 16.23: General disclosure authority in Federal and State proceedings in which the United States is a party.
  o 28 CFR Section 16.24: Procedure in the event of a demand where disclosure is not otherwise authorized.
  o 28 CFR Section 16.25: Final action by the Deputy or Associate Attorney General.
  o 28 CFR Section 16.26: Considerations in determining whether production or disclosure should be made pursuant to a demand.
  o 28 CFR Section 16.27: Procedure in the event a department decision concerning a demand is not made prior to the time a response to the demand is required.
  o 28 CFR Section 16.28: Procedure in the event of an adverse ruling.
  o 28 CFR Section 16.29: Delegation by Assistant Attorneys General.
  o Appendix to Subpart B—Redelegation of Authority to the Deputy Assistant Attorney General for Litigation, Antitrust Division, To Authorize Production or Disclosure of Material or Information

➤ Subpart C—Production of FBI Identification Records in Response to Written Requests by Subjects Thereof
  o 28 CFR Section 16.30: Purpose and scope.
  o 28 CFR Section 16.31: Definition of identification record.
  o 28 CFR Section 16.32: Procedure to obtain an identification record.
  o 28 CFR Section 16.33: Fee for production of identification record.
o 28 CFR Section 16.34: Procedure to obtain change, correction or updating of identification records.

➢ Subpart D—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974

o 28 CFR Section 16.40: General provisions.
o 28 CFR Section 16.41: Requests for access to records.
o 28 CFR Section 16.42: Responsibility for responding to requests for access to records.
o 28 CFR Section 16.43: Responses to requests for access to records.
o 28 CFR Section 16.44: Classified information.
o 28 CFR Section 16.45: Appeals from denials of requests for access to records.
o 28 CFR Section 16.46: Requests for amendment or correction of records.
o 28 CFR Section 16.48: Preservation of records.
o 28 CFR Section 16.49: Fees.
o 28 CFR Section 16.50: Notice of court-ordered and emergency disclosures.
o 28 CFR Section 16.51: Security of systems of records.
o 28 CFR Section 16.52: Contracts for the operation of record systems.
o 28 CFR Section 16.53: Use and collection of social security numbers.
o 28 CFR Section 16.54: Employee standards of conduct.
o 28 CFR Section 16.55: Other rights and services.

➢ Subpart E—Exemption of Records Systems Under the Privacy Act

o 28 CFR Section 16.76: Exemption of Justice Management Division.
o 28 CFR Section 16.77: Exemption of U.S. Trustee Program System—limited access.
o 28 CFR Section 16.79: Exemption of Pardon Attorney System.
- 28 CFR Section 16.82: Exemption of the National Drug Intelligence Center Data Base—limited access.
- 28 CFR Section 16.83: Exemption of the Executive Office for Immigration Review System—limited access.
- 28 CFR Section 16.84: Exemption of Immigration Appeals System.
- 28 CFR Section 16.88: Exemption of Antitrust Division Systems—limited access.
- 28 CFR Section 16.89: Exemption of Civil Division Systems—limited access.
- 28 CFR Section 16.91: Exemption of Criminal Division Systems—limited access, as indicated.
- 28 CFR Section 16.92: Exemption of Environment and Natural Resources Division Systems—limited access.
- 28 CFR Section 16.93: Exemption of Tax Division Systems—limited access.
- 28 CFR Section 16.98: Exemption of the Drug Enforcement Administration (DEA)—limited access.
- 28 CFR Section 16.100: Exemption of Office of Justice Programs—limited access.
- 28 CFR Section 16.101: Exemption of U.S. Marshals Service Systems—limited access, as indicated.
- 28 CFR Section 16.103: Exemption of the INTERPOL-United States National Central Bureau (INTERPOL-USNCB) System.
28 CFR Section 16.130: Exemption of Department of Justice Systems: Correspondence Management Systems for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).

28 CFR Section 16.131: Exemption of Department of Justice (DOJ)/Nationwide Joint Automated Booking System (JABS), DOJ-005.

28 CFR Section 16.132: Exemption of Department of Justice System—Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006.

28 CFR Section 16.133: Exemption of Department of Justice Regional Data Exchange System (RDEX), DOJ-012.

Subpart F—Public Observation of Parole Commission Meetings


28 CFR Section 16.201: Voting by the Commissioners without joint deliberation.


28 CFR Section 16.203: Closed meetings—Formal procedure.

28 CFR Section 16.204: Public notice.

28 CFR Section 16.205: Closed meetings—Informal procedures.

28 CFR Section 16.206: Transcripts, minutes, and miscellaneous documents concerning Commission meetings.

28 CFR Section 16.207: Public access to nonexempt transcripts and minutes of closed Commission meetings—Documents used at meetings—Record retention.

28 CFR Section 16.208: Annual report.

Subpart G—Access to Documents by Former Employees of the Department


28 CFR Section 16.301: Limitations.

Appendix I to Part 16—Components of the Department of Justice

Authority:
SUBPART A—Procedures for Disclosure of Records Under the Freedom of Information Act

Source:
Order No. 2156-98, 63 FR 29593, June 1, 1998, unless otherwise noted.

28 CFR Section 16.1: General provisions.

(a) This subpart contains the rules that the Department of Justice follows in processing requests for records under the Freedom of Information Act (FOIA), 5 U.S.C. 552. These rules should be read together with the FOIA, which provides additional information about access to records maintained by the Department. Requests made by individuals for records about themselves under the Privacy Act of 1974, 5 U.S.C. 552a, which are processed under subpart D of this part, are processed under this subpart also. Information routinely provided to the public as part of a regular Department activity (for example, press releases issued by the Office of Public Affairs) may be provided to the public without following this subpart. As a matter of policy, the Department makes discretionary disclosures of records or information exempt from disclosure under the FOIA whenever disclosure would not foreseeably harm an interest protected by a FOIA exemption, but this policy does not create any right enforceable in court.

(b) As used in this subpart, component means each separate bureau, office, board, division, commission, service, or administration of the Department of Justice.

28 CFR Section 16.2: Public reading rooms.

(a) The Department maintains public reading rooms that contain the records that the FOIA requires to be made regularly available for public inspection and copying. Each Department component is responsible for determining which of the records it generates are required to be made available in this way and for making those records available either in its own reading room or in the Department's central reading room. Each component shall maintain and make available for public inspection and copying a current subject-matter index of its reading room records. Each index shall be updated regularly, at least quarterly, with respect to newly included records.

(b) The Department maintains public reading rooms or areas at the locations listed below:

(1) Bureau of Prisons—on the Seventh Floor, 500 First Street, NW., Washington, DC;
(2) Civil Rights Division—in Room 930, 320 First Street, NW., Washington, DC;

(3) Community Relations Service—in Suite 2000, 600 E Street, NW., Washington, DC;

(4) Drug Enforcement Administration—in Room W-7216, 700 Army Navy Drive, Arlington, Virginia;

(5) Executive Office for Immigration Review (Board of Immigration Appeals)—in Suite 2400, 5107 Leesburg Pike, Falls Church, Virginia;

(6) Federal Bureau of Investigation—at the J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW., Washington, DC;

(7) Foreign Claims Settlement Commission—in Room 6002, 600 E Street, NW., Washington, DC;

(8) Immigration and Naturalization Service—425 I Street, NW., Washington, DC;

(9) Office of Justice Programs—in Room 5430, 810 Seventh Street, NW., Washington, DC;

(10) Pardon Attorney—on the Fourth Floor, 500 First Street, NW., Washington, DC;

(11) Bureau of Alcohol, Tobacco, Firearms, and Explosives—650 Massachusetts Avenue, NW., Washington, DC;

(12) United States Attorneys and United States Marshals—at the principal offices of the United States Attorneys and the United States Marshals, which are listed in most telephone books; and

(13) All other components of the Department of Justice—in Room 6505 at the Main Justice Building, 950 Pennsylvania Avenue, NW., Washington, DC.

(c) Components shall also make reading room records created by the Department on or after November 1, 1996, available electronically at the Department’s World Wide Web site (which can be found at http://www.usdoj.gov), through use of the Department's “Freedom of Information Act Home Page.” This includes each component's index of its reading room records, which will indicate which records are available electronically.
28 CFR Section 16.3: Requirements for making requests.

(a) How made and addressed.
You may make a request for records of the Department of Justice by writing directly to the Department component that maintains those records. You may find the Department's “Freedom of Information Act Reference Guide”—which is available electronically at the Department's World Wide Web site, and is available in paper form as well—helpful in making your request. For additional information about the FOIA, you may refer directly to the statute. If you are making a request for records about yourself, see § 16.41(d) for additional requirements. If you are making a request for records about another individual, either a written authorization signed by that individual permitting disclosure of those records to you or proof that that individual is deceased (for example, a copy of a death certificate or an obituary) will help the processing of your request. Your request should be sent to the component's FOIA office at the address listed in appendix I to part 16. In most cases, your FOIA request should be sent to a component's central FOIA office. For records held by a field office of the Federal Bureau of Investigation (FBI) or the Immigration and Naturalization Service (INS), however, you must write directly to that FBI or INS field office address, which can be found in most telephone books or by calling the component's central FOIA office. (The functions of each component are summarized in part 0 of this title and in the description of the Department and its components in the “United States Government Manual,” which is issued annually and is available in most libraries, as well as for sale from the Government Printing Office's Superintendent of Documents. This manual also can be accessed electronically at the Government Printing Office's World Wide Web site (which can be found at http://www.access.gpo.gov/su_docs).) If you cannot determine where within the Department to send your request, you may send it to the FOIA/PA Mail Referral Unit, Justice Management Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001. That office will forward your request to the component(s) it believes most likely to have the records that you want. Your request will be considered received as of the date it is received by the proper component's FOIA office. For the quickest possible handling, you should mark both your request letter and the envelope “Freedom of Information Act Request.”

(b) Description of records sought.
You must describe the records that you seek in enough detail to enable Department personnel to locate them with a reasonable amount of effort.
Whenever possible, your request should include specific information about each record sought, such as the date, title or name, author, recipient, and subject matter of the record. In addition, if you want records about a court case, you should provide the title of the case, the court in which the case was filed, and the nature of the case. If known, you should include any file designations or descriptions for the records that you want. As a general rule, the more specific you are about the records or type of records that you want, the more likely the Department will be able to locate those records in response to your request. If a component determines that your request does not reasonably describe records, it shall tell you either what additional information is needed or why your request is otherwise insufficient. The component also shall give you an opportunity to discuss your request so that you may modify it to meet the requirements of this section. If your request does not reasonably describe the records you seek, the agency’s response to your request may be delayed.

(c) Agreement to pay fees.
If you make a FOIA request, it shall be considered an agreement by you to pay all applicable fees charged under § 16.11, up to $25.00, unless you seek a waiver of fees. The component responsible for responding to your request ordinarily will confirm this agreement in an acknowledgement letter. When making a request, you may specify a willingness to pay a greater or lesser amount.

Official Citation:
[Order No. 2156-98, 63 FR 29593, June 1, 1998; 63 FR 51401, Sept. 25, 1998]
administrative discretion. If the receiving component determines that it is best able to process the record in response to the request, then it shall do so. If the receiving component determines that it is not best able to process the record, then it shall either:

(1) Respond to the request regarding that record, after consulting with the component or agency best able to determine whether to disclose it and with any other component or agency that has a substantial interest in it; or

(2) Refer the responsibility for responding to the request regarding that record to the component best able to determine whether to disclose it, or to another agency that originated the record (but only if that agency is subject to the FOIA). Ordinarily, the component or agency that originated a record will be presumed to be best able to determine whether to disclose it.

(d) Law enforcement information.
Whenever a request is made for a record containing information that relates to an investigation of a possible violation of law and was originated by another component or agency, the receiving component shall either refer the responsibility for responding to the request regarding that information to that other component or agency or consult with that other component or agency.

(e) Classified information.
Whenever a request is made for a record containing information that has been classified, or may be appropriate for classification, by another component or agency under Executive Order 12958 or any other executive order concerning the classification of records, the receiving component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, should consider the information for classification, or has the primary interest in it, as appropriate. Whenever a record contains information that has been derivatively classified by a component because it contains information classified by another component or agency, the component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the underlying information.

(f) Notice of referral.
Whenever a component refers all or any part of the responsibility for responding to a request to another component or agency, it ordinarily shall notify the requester of the referral and inform the requester of the name of each component or agency to which the request has been referred and of the part of the request that has been referred.

(g) Timing of responses to consultations and referrals.
All consultations and referrals will be handled according to the date the FOIA request initially was received by the first component or agency, not any later date.
(h) Agreements regarding consultations and referrals. Components may make agreements with other components or agencies to eliminate the need for consultations or referrals for particular types of records.

28 CFR Section 16.5: Timing of responses to requests.

(a) In general. Components ordinarily shall respond to requests according to their order of receipt.

(b) Multitrack processing.  
(1) A component may use two or more processing tracks by distinguishing between simple and more complex requests based on the amount of work and/or time needed to process the request, including through limits based on the number of pages involved. If a component does so, it shall advise requesters in its slower track(s) of the limits of its faster track(s).

(2) A component using multitrack processing may provide requesters in its slower track(s) with an opportunity to limit the scope of their requests in order to qualify for faster processing within the specified limits of the component’s faster track(s). A component doing so will contact the requester either by telephone or by letter, whichever is more efficient in each case.

(c) Unusual circumstances.
(1) Where the statutory time limits for processing a request cannot be met because of “unusual circumstances,” as defined in the FOIA, and the component determines to extend the time limits on that basis, the component shall as soon as practicable notify the requester in writing of the unusual circumstances and of the date by which processing of the request can be expected to be completed. Where the extension is for more than ten working days, the component shall provide the requester with an opportunity either to modify the request so that it may be processed within the time limits or to arrange an alternative time period with the component for processing the request or a modified request.

(2) Where a component reasonably believes that multiple requests submitted by a requester, or by a group of requesters acting in concert, constitute a single request that would otherwise involve unusual circumstances, and the requests involve clearly related matters, they may be aggregated. Multiple requests involving unrelated matters will not be aggregated.

(d) Expedited processing.  
(1) Requests and appeals will be taken out of order and given expedited treatment whenever it is determined that they involve:
(i) Circumstances in which the lack of expedited treatment could reasonably be expected to pose an imminent threat to the life or physical safety of an individual;

(ii) An urgency to inform the public about an actual or alleged federal government activity, if made by a person primarily engaged in disseminating information;

(iii) The loss of substantial due process rights; or

(iv) A matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence.

(2) A request for expedited processing may be made at the time of the initial request for records or at any later time. For a prompt determination, a request for expedited processing must be received by the proper component. Requests based on the categories in paragraphs (d)(1)(i), (ii), and (iii) of this section must be submitted to the component that maintains the records requested. Requests based on the category in paragraph (d)(1)(iv) of this section must be submitted to the Director of Public Affairs, whose address is: Office of Public Affairs, U.S. Department of Justice, Room 1128, 950 Pennsylvania Avenue, NW., Washington DC 20530-0001. A component that receives a request that must be handled by the Office of Public Affairs shall forward it immediately to that office by hand-delivery or fax.

(3) A requester who seeks expedited processing must submit a statement, certified to be true and correct to the best of that person's knowledge and belief, explaining in detail the basis for requesting expedited processing. For example, a requester within the category in paragraph (d)(1)(ii) of this section, if not a full-time member of the news media, must establish that he or she is a person whose main professional activity or occupation is information dissemination, though it need not be his or her sole occupation. A requester within the category in paragraph (d)(1)(ii) of this section also must establish a particular urgency to inform the public about the government activity involved in the request, beyond the public's right to know about government activity generally. The formality of certification may be waived as a matter of administrative discretion.

(4) Within ten calendar days of its receipt of a request for expedited processing, the proper component shall decide whether to grant it and shall notify the requester of the decision. If a request for expedited treatment is granted, the request shall be given priority and shall be processed as soon as practicable. If a request for expedited processing is denied, any appeal of that decision shall be acted on expeditiously.
28 CFR Section 16.6: Responses to requests.

(a) Acknowledgements of requests.
On receipt of a request, a component ordinarily shall send an acknowledgement letter to the requester which shall confirm the requester’s agreement to pay fees under § 16.3(c) and provide an assigned request number for further reference.

(b) Grants of requests.
Ordinarily, a component shall have twenty business days from when a request is received to determine whether to grant or deny the request. Once a component makes a determination to grant a request in whole or in part, it shall notify the requester in writing. The component shall inform the requester in the notice of any fee charged under § 16.11 and shall disclose records to the requester promptly on payment of any applicable fee. Records disclosed in part shall be marked or annotated to show the amount of information deleted unless doing so would harm an interest protected by an applicable exemption. The location of the information deleted also shall be indicated on the record, if technically feasible.

(c) Adverse determinations of requests.
A component making an adverse determination denying a request in any respect shall notify the requester of that determination in writing. Adverse determinations, or denials of requests, consist of: a determination to withhold any requested record in whole or in part; a determination that a requested record does not exist or cannot be located; a determination that a record is not readily reproducible in the form or format sought by the requester; a determination that what has been requested is not a record subject to the FOIA; a determination on any disputed fee matter, including a denial of a request for a fee waiver; and a denial of a request for expedited treatment. The denial letter shall be signed by the head of the component, or the component head's designee, and shall include:

(1) The name and title or position of the person responsible for the denial;

(2) A brief statement of the reason(s) for the denial, including any FOIA exemption applied by the component in denying the request;

(3) An estimate of the volume of records or information withheld, in number of pages or in some other reasonable form of estimation. This estimate does not need to be provided if the volume is otherwise indicated through deletions on records disclosed in part, or if providing an estimate would harm an interest protected by an applicable exemption; and
(4) A statement that the denial may be appealed under § 16.9(a) and a
description of the requirements of § 16.9(a).

28 CFR Section 16.7: Classified information.

In processing a request for information that is classified under Executive Order 12958 (3 CFR, 1996 Comp., p. 333) or any other executive order, the originating component shall review the information to determine whether it should remain classified. Information determined to no longer require classification shall not be withheld on the basis of Exemption 1 of the FOIA. On receipt of any appeal involving classified information, the Office of Information and Privacy shall take appropriate action to ensure compliance with part 17 of this title.

28 CFR Section 16.8: Business information.

(a) In general.
Business information obtained by the Department from a submitter will be disclosed under the FOIA only under this section.

(b) Definitions.
For purposes of this section:

(1) Business information
means commercial or financial information obtained by the Department from a submitter that may be protected from disclosure under Exemption 4 of the FOIA.

(2) Submitter
means any person or entity from whom the Department obtains business information, directly or indirectly. The term includes corporations; state, local, and tribal governments; and foreign governments.

(c) Designation of business information.
A submitter of business information will use good-faith efforts to designate, by appropriate markings, either at the time of submission or at a reasonable time thereafter, any portions of its submission that it considers to be protected from disclosure under Exemption 4. These designations will expire ten years after the date of the submission unless the submitter requests, and provides justification for, a longer designation period.

(d) Notice to submitters.
A component shall provide a submitter with prompt written notice of a FOIA request or administrative appeal that seeks its business information wherever required under paragraph (e) of this section, except as provided in paragraph (h) of this section, in order to give the submitter an opportunity to object to disclosure of any specified portion of that information under paragraph (f) of this section. The notice shall either describe the business information requested or include copies of the requested records or record portions containing the information. When notification of a voluminous number of submitters is required, notification may be made by posting or publishing the notice in a place reasonably likely to accomplish it.

(e) Where notice is required.
Notice shall be given to a submitter wherever:

1. The information has been designated in good faith by the submitter as information considered protected from disclosure under Exemption 4; or

2. The component has reason to believe that the information may be protected from disclosure under Exemption 4.

(f) Opportunity to object to disclosure.
A component will allow a submitter a reasonable time to respond to the notice described in paragraph (d) of this section and will specify that time period within the notice. If a submitter has any objection to disclosure, it is required to submit a detailed written statement. The statement must specify all grounds for withholding any portion of the information under any exemption of the FOIA and, in the case of Exemption 4, it must show why the information is a trade secret or commercial or financial information that is privileged or confidential. In the event that a submitter fails to respond to the notice within the time specified in it, the submitter will be considered to have no objection to disclosure of the information. Information provided by the submitter that is not received by the component until after its disclosure decision has been made shall not be considered by the component. Information provided by a submitter under this paragraph may itself be subject to disclosure under the FOIA.

(g) Notice of intent to disclose.
A component shall consider a submitter's objections and specific grounds for nondisclosure in deciding whether to disclose business information. Whenever a component decides to disclose business information over the objection of a submitter, the component shall give the submitter written notice, which shall include:

1. A statement of the reason(s) why each of the submitter's disclosure objections was not sustained;

2. A description of the business information to be disclosed; and
(3) A specified disclosure date, which shall be a reasonable time subsequent to the notice.

(h) Exceptions to notice requirements.
The notice requirements of paragraphs (d) and (g) of this section shall not apply if:

(1) The component determines that the information should not be disclosed;

(2) The information lawfully has been published or has been officially made available to the public;

(3) Disclosure of the information is required by statute (other than the FOIA) or by a regulation issued in accordance with the requirements of Executive Order 12600 (3 CFR, 1988 Comp., p. 235); or

(4) The designation made by the submitter under paragraph (c) of this section appears obviously frivolous—except that, in such a case, the component shall, within a reasonable time prior to a specified disclosure date, give the submitter written notice of any final decision to disclose the information.

(i) Notice of FOIA lawsuit.
Whenever a requester files a lawsuit seeking to compel the disclosure of business information, the component shall promptly notify the submitter.

(j) Corresponding notice to requesters.
Whenever a component provides a submitter with notice and an opportunity to object to disclosure under paragraph (d) of this section, the component shall also notify the requester(s). Whenever a component notifies a submitter of its intent to disclose requested information under paragraph (g) of this section, the component shall also notify the requester(s). Whenever a submitter files a lawsuit seeking to prevent the disclosure of business information, the component shall notify the requester(s).

Official Citation:
[Order No. 2156-98, 63 FR 29593, June 1, 1998; 63 FR 51401, Sept. 25, 1998]

28 CFR Section 16.9: Appeals.

(a) Appeals of adverse determinations.
If you are dissatisfied with a component's response to your request, you may appeal an adverse determination denying your request, in any respect, to the
Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, DC 20530-0001. You must make your appeal in writing and it must be received by the Office of Information and Privacy within 60 days of the date of the letter denying your request. Your appeal letter may include as much or as little related information as you wish, as long as it clearly identifies the component determination (including the assigned request number, if known) that you are appealing. For the quickest possible handling, you should mark your appeal letter and the envelope “Freedom of Information Act Appeal.” Unless the Attorney General directs otherwise, a Director of the Office of Information and Privacy will act on behalf of the Attorney General on all appeals under this section, except that:

(1) In the case of an adverse determination by the Deputy Attorney General or the Associate Attorney General, the Attorney General or the Attorney General’s designee will act on the appeal;

(2) An adverse determination by the Attorney General will be the final action of the Department; and

(3) An appeal ordinarily will not be acted on if the request becomes a matter of FOIA litigation.

(b) Responses to appeals.
The decision on your appeal will be made in writing. A decision affirming an adverse determination in whole or in part shall contain a statement of the reason(s) for the affirmance, including any FOIA exemption(s) applied, and will inform you of the FOIA provisions for court review of the decision. If the adverse determination is reversed or modified on appeal, in whole or in part, you will be notified in a written decision and your request will be reprocessed in accordance with that appeal decision.

(c) When appeal is required.
If you wish to seek review by a court of any adverse determination, you must first appeal it under this section.

28 CFR Section 16.10: Preservation of records.

Each component shall preserve all correspondence pertaining to the requests that it receives under this subpart, as well as copies of all requested records, until disposition or destruction is authorized by title 44 of the United States Code or the National Archives and Records Administration’s General Records Schedule 14. Records will not be disposed of while they are the subject of a pending request, appeal, or lawsuit under the FOIA.
28 CFR Section 16.11: Fees.

(a) In general.
Components shall charge for processing requests under the FOIA in accordance with paragraph (c) of this section, except where fees are limited under paragraph (d) of this section or where a waiver or reduction of fees is granted under paragraph (k) of this section. A component ordinarily shall collect all applicable fees before sending copies of requested records to a requester. Requesters must pay fees by check or money order made payable to the Treasury of the United States.

(b) Definitions.
For purposes of this section:

(1) Commercial use request
means a request from or on behalf of a person who seeks information for a use or purpose that furthers his or her commercial, trade, or profit interests, which can include furthering those interests through litigation. Components shall determine, whenever reasonably possible, the use to which a requester will put the requested records. When it appears that the requester will put the records to a commercial use, either because of the nature of the request itself or because a component has reasonable cause to doubt a requester's stated use, the component shall provide the requester a reasonable opportunity to submit further clarification.

(2) Direct costs
means those expenses that an agency actually incurs in searching for and duplicating (and, in the case of commercial use requests, reviewing) records to respond to a FOIA request. Direct costs include, for example, the salary of the employee performing the work (the basic rate of pay for the employee, plus 16 percent of that rate to cover benefits) and the cost of operating duplication machinery. Not included in direct costs are overhead expenses such as the costs of space and heating or lighting of the facility in which the records are kept.

(3) Duplication
means the making of a copy of a record, or of the information contained in it, necessary to respond to a FOIA request. Copies can take the form of paper, microform, audiovisual materials, or electronic records (for example, magnetic tape or disk), among others. Components shall honor a requester's specified preference of form or format of disclosure if the record is readily reproducible.
with reasonable efforts in the requested form or format by the office responding to the request.

(4) **Educational institution**
means a preschool, a public or private elementary or secondary school, an institution of undergraduate higher education, an institution of graduate higher education, an institution of professional education, or an institution of vocational education, that operates a program of scholarly research. To be in this category, a requester must show that the request is authorized by and is made under the auspices of a qualifying institution and that the records are not sought for a commercial use but are sought to further scholarly research.

(5) **Noncommercial scientific institution**
means an institution that is not operated on a “commercial” basis, as that term is defined in paragraph (b)(1) of this section, and that is operated solely for the purpose of conducting scientific research the results of which are not intended to promote any particular product or industry. To be in this category, a requester must show that the request is authorized by and is made under the auspices of a qualifying institution and that the records are not sought for a commercial use but are sought to further scientific research.

(6) **Representative of the news media, or news media requester**
means any person actively gathering news for an entity that is organized and operated to publish or broadcast news to the public. The term “news” means information that is about current events or that would be of current interest to the public. Examples of news media entities include television or radio stations broadcasting to the public at large and publishers of periodicals (but only in those instances where they can qualify as disseminators of “news”) who make their products available for purchase or subscription by the general public. For “freelance” journalists to be regarded as working for a news organization, they must demonstrate a solid basis for expecting publication through that organization. A publication contract would be the clearest proof, but components shall also look to the past publication record of a requester in making this determination. To be in this category, a requester must not be seeking the requested records for a commercial use. However, a request for records supporting the news-dissemination function of the requester shall not be considered to be for a commercial use.

(7) **Review**
means the examination of a record located in response to a request in order to determine whether any portion of it is exempt from disclosure. It also includes processing any record for disclosure—for example, doing all that is necessary to redact it and prepare it for disclosure. Review costs are recoverable even if a
record ultimately is not disclosed. Review time includes time spent considering any formal objection to disclosure made by a business submitter under § 16.8, but does not include time spent resolving general legal or policy issues regarding the application of exemptions.

(8) Search
means the process of looking for and retrieving records or information responsive to a request. It includes page-by-page or line-by-line identification of information within records and also includes reasonable efforts to locate and retrieve information from records maintained in electronic form or format. Components shall ensure that searches are done in the most efficient and least expensive manner reasonably possible. For example, components shall not search line-by-line where duplicating an entire document would be quicker and less expensive.

(c) Fees.
In responding to FOIA requests, components shall charge the following fees unless a waiver or reduction of fees has been granted under paragraph (k) of this section:

(i) Search.
Search fees shall be charged for all requests—other than requests made by educational institutions, noncommercial scientific institutions, or representatives of the news media—subject to the limitations of paragraph (d) of this section. Components may charge for time spent searching even if they do not locate any responsive record or if they withhold the record(s) located as entirely exempt from disclosure.

(ii) For each quarter hour spent by clerical personnel in searching for and retrieving a requested record, the fee will be $4.00. Where a search and retrieval cannot be performed entirely by clerical personnel—for example, where the identification of records within the scope of a request requires the use of professional personnel—the fee will be $7.00 for each quarter hour of search time spent by professional personnel. Where the time of managerial personnel is required, the fee will be $10.25 for each quarter hour of time spent by those personnel.

(iii) For computer searches of records, requesters will be charged the direct costs of conducting the search, although certain requesters (as provided in paragraph (d)(1) of this section) will be charged no search fee and certain other requesters (as provided in paragraph (d)(3) of this section) will be entitled to the cost equivalent of two hours of manual search time without charge. These direct costs will include the cost of operating a central processing unit for that portion of operating time that is directly attributable to searching for
responsive records, as well as the costs of operator/programmer salary apportionable to the search.

(2) Duplication. Duplication fees will be charged to all requesters, subject to the limitations of paragraph (d) of this section. For a paper photocopy of a record (no more than one copy of which need be supplied), the fee will be ten cents per page. For copies produced by computer, such as tapes or printouts, components will charge the direct costs, including operator time, of producing the copy. For other forms of duplication, components will charge the direct costs of that duplication.

(3) Review. Review fees will be charged to requesters who make a commercial use request. Review fees will be charged only for the initial record review—in other words, the review done when a component determines whether an exemption applies to a particular record or record portion at the initial request level. No charge will be made for review at the administrative appeal level for an exemption already applied. However, records or record portions withheld under an exemption that is subsequently determined not to apply may be reviewed again to determine whether any other exemption not previously considered applies; the costs of that review are chargeable where it is made necessary by such a change of circumstances. Review fees will be charged at the same rates as those charged for a search under paragraph (c)(1)(ii) of this section.

(d) Limitations on charging fees. (1) No search fee will be charged for requests by educational institutions, noncommercial scientific institutions, or representatives of the news media.

(2) No search fee or review fee will be charged for a quarter-hour period unless more than half of that period is required for search or review.

(3) Except for requesters seeking records for a commercial use, components will provide without charge:

   (i) The first 100 pages of duplication (or the cost equivalent); and

   (ii) The first two hours of search (or the cost equivalent).

(4) Whenever a total fee calculated under paragraph (c) of this section is $14.00 or less for any request, no fee will be charged.

(5) The provisions of paragraphs (d) (3) and (4) of this section work together. This means that for requesters other than those seeking records for a
commercial use, no fee will be charged unless the cost of search in excess of two
hours plus the cost of duplication in excess of 100 pages totals more than $14.00.

(e) Notice of anticipated fees in excess of $25.00.
When a component determines or estimates that the fees to be charged under
this section will amount to more than $25.00, the component shall notify the
requester of the actual or estimated amount of the fees, unless the requester has
indicated a willingness to pay fees as high as those anticipated. If only a portion
of the fee can be estimated readily, the component shall advise the requester that
the estimated fee may be only a portion of the total fee. In cases in which a
requester has been notified that actual or estimated fees amount to more than
$25.00, the request shall not be considered received and further work shall not
be done on it until the requester agrees to pay the anticipated total fee. Any such
agreement should be memorialized in writing. A notice under this paragraph will
offer the requester an opportunity to discuss the matter with Department
personnel in order to reformulate the request to meet the requester’s needs at a
lower cost.

(f) Charges for other services.
Apart from the other provisions of this section, when a component chooses as a
matter of administrative discretion to provide a special service—such as certifying
that records are true copies or sending them by other than ordinary mail—the
direct costs of providing the service ordinarily will be charged.

(g) Charging interest.
Components may charge interest on any unpaid bill starting on the 31st day
following the date of billing the requester. Interest charges will be assessed at the
rate provided in 31 U.S.C. 3717 and will accrue from the date of the billing until
payment is received by the component. Components will follow the provisions of
the Debt Collection Act of 1982 (Pub. L. 97-365, 96 Stat. 1749), as amended, and
its administrative procedures, including the use of consumer reporting agencies,
collection agencies, and offset.

(h) Aggregating requests.
Where a component reasonably believes that a requester or a group of requesters
acting together is attempting to divide a request into a series of requests for the
purpose of avoiding fees, the component may aggregate those requests and
charge accordingly. Components may presume that multiple requests of this type
made within a 30-day period have been made in order to avoid fees. Where
requests are separated by a longer period, components will aggregate them only
where there exists a solid basis for determining that aggregation is warranted
under all the circumstances involved. Multiple requests involving unrelated
matters will not be aggregated.

(i) Advance payments.
(1) For requests other than those described in paragraphs (i)(2) and (3) of this section, a component shall not require the requester to make an advance payment—in other words, a payment made before work is begun or continued on a request. Payment owed for work already completed (i.e., a prepayment before copies are sent to a requester) is not an advance payment.

(2) Where a component determines or estimates that a total fee to be charged under this section will be more than $250.00, it may require the requester to make an advance payment of an amount up to the amount of the entire anticipated fee before beginning to process the request, except where it receives a satisfactory assurance of full payment from a requester that has a history of prompt payment.

(3) Where a requester has previously failed to pay a properly charged FOIA fee to any component or agency within 30 days of the date of billing, a component may require the requester to pay the full amount due, plus any applicable interest, and to make an advance payment of the full amount of any anticipated fee, before the component begins to process a new request or continues to process a pending request from that requester.

(4) In cases in which a component requires advance payment or payment due under paragraph (i)(2) or (3) of this section, the request shall not be considered received and further work will not be done on it until the required payment is received.

(j) Other statutes specifically providing for fees.
The fee schedule of this section does not apply to fees charged under any statute that specifically requires an agency to set and collect fees for particular types of records. Where records responsive to requests are maintained for distribution by agencies operating such statutorily based fee schedule programs, components will inform requesters of the steps for obtaining records from those sources so that they may do so most economically.

(k) Requirements for waiver or reduction of fees.
(1) Records responsive to a request will be furnished without charge or at a charge reduced below that established under paragraph (c) of this section where a component determines, based on all available information, that the requester has demonstrated that:

(i) Disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government, and

(ii) Disclosure of the information is not primarily in the commercial interest of the requester.
(2) To determine whether the first fee waiver requirement is met, components will consider the following factors:

   (i) The subject of the request: Whether the subject of the requested records concerns “the operations or activities of the government.” The subject of the requested records must concern identifiable operations or activities of the federal government, with a connection that is direct and clear, not remote or attenuated.

   (ii) The informative value of the information to be disclosed: Whether the disclosure is “likely to contribute” to an understanding of government operations or activities. The disclosable portions of the requested records must be meaningfully informative about government operations or activities in order to be “likely to contribute” to an increased public understanding of those operations or activities. The disclosure of information that already is in the public domain, in either a duplicative or a substantially identical form, would not be as likely to contribute to such understanding where nothing new would be added to the public’s understanding.

   (iii) The contribution to an understanding of the subject by the public likely to result from disclosure: Whether disclosure of the requested information will contribute to “public understanding.” The disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester. A requester’s expertise in the subject area and ability and intention to effectively convey information to the public shall be considered. It shall be presumed that a representative of the news media will satisfy this consideration.

   (iv) The significance of the contribution to public understanding: Whether the disclosure is likely to contribute “significantly” to public understanding of government operations or activities. The public’s understanding of the subject in question, as compared to the level of public understanding existing prior to the disclosure, must be enhanced by the disclosure to a significant extent. Components shall not make value judgments about whether information that would contribute significantly to public understanding of the operations or activities of the government is “important” enough to be made public.

(3) To determine whether the second fee waiver requirement is met, components will consider the following factors:

   (i) The existence and magnitude of a commercial interest: Whether the requester has a commercial interest that would be furthered by the requested disclosure.
Components shall consider any commercial interest of the requester (with reference to the definition of “commercial use” in paragraph (b)(1) of this section), or of any person on whose behalf the requester may be acting, that would be furthered by the requested disclosure. Requesters shall be given an opportunity in the administrative process to provide explanatory information regarding this consideration.

(ii) The primary interest in disclosure: Whether any identified commercial interest of the requester is sufficiently large, in comparison with the public interest in disclosure, that disclosure is “primarily in the commercial interest of the requester.”

A fee waiver or reduction is justified where the public interest standard is satisfied and that public interest is greater in magnitude than that of any identified commercial interest in disclosure. Components ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester. Disclosure to data brokers or others who merely compile and market government information for direct economic return shall not be presumed to primarily serve the public interest.

(4) Where only some of the records to be released satisfy the requirements for a waiver of fees, a waiver shall be granted for those records.

(5) Requests for the waiver or reduction of fees should address the factors listed in paragraphs (k)(2) and (3) of this section, insofar as they apply to each request. Components will exercise their discretion to consider the cost-effectiveness of their investment of administrative resources in this decisionmaking process, however, in deciding to grant waivers or reductions of fees.

Official Citation:

28 CFR Section 16.12: Other rights and services.

Nothing in this subpart shall be construed to entitle any person, as of right, to any service or to the disclosure of any record to which such person is not entitled under the FOIA.
SUBPART B—Production or Disclosure in Federal and State Proceedings

Source:
Order No. 919-80, 45 FR 83210, Dec. 18, 1980, unless otherwise noted.

28 CFR Section 16.21: Purpose and scope.

(a) This subpart sets forth procedures to be followed with respect to the production or disclosure of any material contained in the files of the Department, any information relating to material contained in the files of the Department, or any information acquired by any person while such person was an employee of the Department as a part of the performance of that person’s official duties or because of that person’s official status:

(1) In all federal and state proceedings in which the United States is a party; and

(2) In all federal and state proceedings in which the United States is not a party, including any proceedings in which the Department is representing a government employee solely in that employee’s individual capacity, when a subpoena, order, or other demand (hereinafter collectively referred to as a “demand”) of a court or other authority is issued for such material or information.

(b) For purposes of this subpart, the term employee of the Department includes all officers and employees of the United States appointed by, or subject to the supervision, jurisdiction, or control of the Attorney General of the United States, including U.S. Attorneys, U.S. Marshals, U.S. Trustees and members of the staffs of those officials.

(c) Nothing in this subpart is intended to impede the appropriate disclosure, in the absence of a demand, of information by Department law enforcement agencies to federal, state, local and foreign law enforcement, prosecutive, or regulatory agencies.

(d) This subpart is intended only to provide guidance for the internal operations of the Department of Justice, and is not intended to, and does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States.
28 CFR Section 16.22: General prohibition of production or disclosure in Federal and State proceedings in which the United States is not a party.

(a) In any federal or state case or matter in which the United States is not a party, no employee or former employee of the Department of Justice shall, in response to a demand, produce any material contained in the files of the Department, or disclose any information relating to or based upon material contained in the files of the Department, or disclose any information or produce any material acquired as part of the performance of that person’s official duties or because of that person’s official status without prior approval of the proper Department official in accordance with §§ 16.24 and 16.25 of this part.

(b) Whenever a demand is made upon an employee or former employee as described in paragraph (a) of this section, the employee shall immediately notify the U.S. Attorney for the district where the issuing authority is located. The responsible United States Attorney shall follow procedures set forth in § 16.24 of this part.

(c) If oral testimony is sought by a demand in any case or matter in which the United States is not a party, an affidavit, or, if that is not feasible, a statement by the party seeking the testimony or by his attorney, setting forth a summary of the testimony sought and its relevance to the proceeding, must be furnished to the responsible U.S. Attorney. Any authorization for testimony by a present or former employee of the Department shall be limited to the scope of the demand as summarized in such statement.

(d) When information other than oral testimony is sought by a demand, the responsible U.S. Attorney shall request a summary of the information sought and its relevance to the proceeding.

28 CFR Section 16.23: General disclosure authority in Federal and State proceedings in which the United States is a party.

(a) Every attorney in the Department of Justice in charge of any case or matter in which the United States is a party is authorized, after consultation with the “originating component” as defined in § 16.24(a) of this part, to reveal and furnish to any person, including an actual or prospective witness, a grand jury, counsel, or a court, either during or preparatory to a proceeding, such testimony, and relevant unclassified material, documents, or information secured by any attorney, or investigator of the Department of Justice, as such attorney shall deem necessary or desirable to the discharge of the attorney’s official duties: Provided, Such an attorney shall consider, with respect to any disclosure, the factors set forth in § 16.26(a) of this part: And further provided, an attorney shall
not reveal or furnish any material, documents, testimony or information when, in the attorney's judgment, any of the factors specified in § 16.26(b) exists, without the express prior approval by the Assistant Attorney General in charge of the division responsible for the case or proceeding, the Director of the Executive Office for United States Trustees (hereinafter referred to as “the EOUST”), or such persons' designees.

(b) An attorney may seek higher level review at any stage of a proceeding, including prior to the issuance of a court order, when the attorney determines that a factor specified in § 16.26(b) exists or foresees that higher level approval will be required before disclosure of the information or testimony in question. Upon referral of a matter under this subsection, the responsible Assistant Attorney General, the Director of EOUST, or their designees shall follow procedures set forth in § 16.24 of this part.

(c) If oral testimony is sought by a demand in a case or matter in which the United States is a party, an affidavit, or, if that is not feasible, a statement by the party seeking the testimony or by the party's attorney setting forth a summary of the testimony sought must be furnished to the Department attorney handling the case or matter.

28 CFR Section 16.24: Procedure in the event of a demand where disclosure is not otherwise authorized.

(a) Whenever a matter is referred under § 16.22 of this part to a U.S. Attorney or, under § 16.23 of this part, to an Assistant Attorney General, the Director of the EOUST, or their designees (hereinafter collectively referred to as the “responsible official”), the responsible official shall immediately advise the official in charge of the bureau, division, office, or agency of the Department that was responsible for the collection, assembly, or other preparation of the material demanded or that, at the time the person whose testimony was demanded acquired the information in question, employed such person (hereinafter collectively referred to as the “originating component”), or that official's designee. In any instance in which the responsible official is also the official in charge of the originating component, the responsible official may perform all functions and make all determinations that this regulation vests in the originating component.

(b) The responsible official, subject to the terms of paragraph (c) of this section, may authorize the appearance and testimony of a present or former Department employee, or the production of material from Department files if:

(1) There is no objection after inquiry of the originating component;
(2) The demanded disclosure, in the judgment of the responsible official, is appropriate under the factors specified in § 16.26(a) of this part; and

(3) None of the factors specified in § 16.26(b) of this part exists with respect to the demanded disclosure.

c) It is Department policy that the responsible official shall, following any necessary consultation with the originating component, authorize testimony by a present or former employee of the Department or the production of material from Department files without further authorization from Department officials whenever possible: Provided, that, when information is collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of the Department or by the EOUST, the Assistant Attorney General in charge of such a division or the Director of the EOUST may require that the originating component obtain the division's or the EOUST's approval before authorizing a responsible official to disclose such information. Prior to authorizing such testimony or production, however, the responsible official shall, through negotiation and, if necessary, appropriate motions, seek to limit the demand to information, the disclosure of which would not be inconsistent with the considerations specified in § 16.26 of this part.

(d)(1) In a case in which the United States is not a party, if the responsible U.S. attorney and the originating component disagree with respect to the appropriateness of demanded testimony or of a particular disclosure, or if they agree that such testimony or such a disclosure should not be made, they shall determine if the demand involves information that was collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of this Department or the EOUST. If so, the U.S. attorney shall notify the Director of the EOUST or the Assistant Attorney General in charge of the division responsible for such litigation or investigation, who may:

(i) Authorize personally or through a Deputy Assistant Attorney General, the demanded testimony or other disclosure of the information if such testimony or other disclosure, in the Assistant or Deputy Assistant Attorney General's judgment or in the judgment of the Director of the EOUST, is consistent with the factors specified in § 16.26(a) of this part, and none of the factors specified in § 16.26(b) of this part exists with respect to the demanded disclosure;

(ii) Authorize, personally or by a designee, the responsible official, through negotiations and, if necessary, appropriate motions, to seek to limit the demand to matters, the disclosure of which, through testimony or documents, considerations specified in § 16.26 of this part, and otherwise to take all appropriate steps to limit the scope or obtain the withdrawal of a demand; or
(iii) If, after all appropriate steps have been taken to limit the scope or obtain the withdrawal of a demand, the Director of the EOUST or the Assistant or Deputy Assistant Attorney General does not authorize the demanded testimony or other disclosure, refer the matter, personally or through a Deputy Assistant Attorney General, for final resolution to the Deputy or Associate Attorney General, as indicated in § 16.25 of this part.

(2) If the demand for testimony or other disclosure in such a case does not involve information that was collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of this Department, the originating component shall decide whether disclosure is appropriate, except that, when especially significant issues are raised, the responsible official may refer the matter to the Deputy or Associate Attorney General, as indicated in § 16.25 of this part. If the originating component determines that disclosure would not be appropriate and the responsible official does not refer the matter for higher level review, the responsible official shall take all appropriate steps to limit the scope or obtain the withdrawal of a demand.

(e) In a case in which the United States is a party, the Assistant General or the Director of the EOUST responsible for the case or matter, or such persons' designees, are authorized, after consultation with the originating component, to exercise the authorities specified in paragraph (d)(1) (i) through (iii) of this section: Provided, that if a demand involves information that was collected, assembled, or prepared originally in connection with litigation or an investigation supervised by another unit of the Department, the responsible official shall notify the other division or the EOUST concerning the demand and the anticipated response. If two litigating units of the Department are unable to resolve a disagreement concerning disclosure, the Assistant Attorneys General in charge of the two divisions in disagreement, or the Director of the EOUST and the appropriate Assistant Attorney General, may refer the matter to the Deputy or Associate Attorney General, as indicated in § 16.25(b) of this part.

(f) In any case or matter in which the responsible official and the originating component agree that it would not be appropriate to authorize testimony or otherwise to disclose the information demanded, even if a court were so to require, no Department attorney responding to the demand should make any representation that implies that the Department would, in fact, comply with the demand if directed to do so by a court. After taking all appropriate steps in such cases to limit the scope or obtain the withdrawal of a demand, the responsible official shall refer the matter to the Deputy or Associate Attorney General, as indicated in § 16.25 of this part.

(g) In any case or matter in which the Attorney General is personally involved in the claim of privilege, the responsible official may consult with the Attorney
General and proceed in accord with the Attorney General’s instructions without subsequent review by the Deputy or Associate Attorney General.

28 CFR Section 16.25: Final action by the Deputy or Associate Attorney General.

(a) Unless otherwise indicated, all matters to be referred under § 16.24 by an Assistant Attorney General, the Director of the EOUST, or such person’s designees to the Deputy or Associate Attorney General shall be referred (1) to the Deputy Attorney General, if the matter is referred personally by or through the designee of an Assistant Attorney General who is within the general supervision of the Deputy Attorney General, or (2) to the Associate Attorney General, in all other cases.

(b) All other matters to be referred under § 16.24 to the Deputy or Associate Attorney General shall be referred (1) to the Deputy Attorney General, if the originating component is within the supervision of the Deputy Attorney General or is an independent agency that, for administrative purposes, is within the Department of Justice, or (2) to the Associate Attorney General, if the originating component is within the supervision of the Associate Attorney General.

(c) Upon referral, the Deputy or Associate Attorney General shall make the final decision and give notice thereof to the responsible official and such other persons as circumstances may warrant.

28 CFR Section 16.26: Considerations in determining whether production or disclosure should be made pursuant to a demand.

(a) In deciding whether to make disclosures pursuant to a demand, Department officials and attorneys should consider:

(1) Whether such disclosure is appropriate under the rules of procedure governing the case or matter in which the demand arose, and

(2) Whether disclosure is appropriate under the relevant substantive law concerning privilege.

(b) Among the demands in response to which disclosure will not be made by any Department official are those demands with respect to which any of the following factors exist:
(1) Disclosure would violate a statute, such as the income tax laws, 26 U.S.C. 6103 and 7213, or a rule of procedure, such as the grand jury secrecy rule, F.R.Cr.P., Rule 6(e),

(2) Disclosure would violate a specific regulation;

(3) Disclosure would reveal classified information, unless appropriately declassified by the originating agency,

(4) Disclosure would reveal a confidential source or informant, unless the investigative agency and the source or informant have no objection,

(5) Disclosure would reveal investigatory records compiled for law enforcement purposes, and would interfere with enforcement proceedings or disclose investigative techniques and procedures the effectiveness of which would thereby be impaired,

(6) Disclosure would improperly reveal trade secrets without the owner's consent.

(c) In all cases not involving considerations specified in paragraphs (b)(1) through (b)(6) of this section, the Deputy or Associate Attorney General will authorize disclosure unless, in that person's judgment, after considering paragraph (a) of this section, disclosure is unwarranted. The Deputy or Associate Attorney General will not approve disclosure if the circumstances specified in paragraphs (b)(1) through (b)(3) of this section exist. The Deputy or Associate Attorney General will not approve disclosure if any of the conditions in paragraphs (b)(4) through (b)(6) of this section exist, unless the Deputy or Associate Attorney General determines that the administration of justice requires disclosure. In this regard, if disclosure is necessary to pursue a civil or criminal prosecution or affirmative relief, such as an injunction, consideration shall be given to:

(1) The seriousness of the violation or crime involved,

(2) The past history or criminal record of the violator or accused,

(3) The importance of the relief sought,

(4) The importance of the legal issues presented,

(5) Other matters brought to the attention of the Deputy or Associate Attorney General.
(d) Assistant Attorneys General, U.S. Attorneys, the Director of the EOUST, U.S. Trustees, and their designees, are authorized to issue instructions to attorneys and to adopt supervisory practices, consistent with this subpart, in order to help foster consistent application of the foregoing standards and the requirements of this subpart.

28 CFR Section 16.27: Procedure in the event a department decision concerning a demand is not made prior to the time a response to the demand is required.

If response to a demand is required before the instructions from the appropriate Department official are received, the responsible official or other Department attorney designated for the purpose shall appear and furnish the court or other authority with a copy of the regulations contained in this subpart and inform the court or other authority that the demand has been or is being, as the case may be, referred for the prompt consideration of the appropriate Department official and shall respectfully request the court or authority to stay the demand pending receipt of the requested instructions.

28 CFR Section 16.28: Procedure in the event of an adverse ruling.

If the court or other authority declines to stay the effect of the demand in response to a request made in accordance with § 16.27 of this chapter pending receipt of instructions, or if the court or other authority rules that the demand must be complied with irrespective of instructions rendered in accordance with §§ 16.24 and 16.25 of this part not to produce the material or disclose the information sought, the employee or former employee upon whom the demand has been made shall, if so directed by the responsible Department official, respectfully decline to comply with the demand. See United States ex rel. Touhy v. Ragen, 340 U.S. 462 (1951).

28 CFR Section 16.29: Delegation by Assistant Attorneys General.

With respect to any function that this subpart permits the designee of an Assistant Attorney General to perform, the Assistant Attorneys General are authorized to delegate their authority, in any case or matter or any category of cases or matters, to subordinate division officials or U.S. attorneys, as appropriate.
Appendix to SUBPART B of Part 16—Redelegation of Authority to the Deputy Assistant Attorney General for Litigation, Antitrust Division, To Authorize Production or Disclosure of Material or Information

1. By virtue of the authority vested in me by 28 CFR 16.23(b)(1) the authority delegated to me by that section to authorize the production of material and disclosure of information described in 28 CFR 16.21(a) is hereby redelegated to the Deputy Assistant Attorney General for Litigation, Antitrust Division.

2. This directive shall become effective on the date of its publication in the Federal Register.

Official Citation:
[Order No. 960-81, 46 FR 52356, Oct. 27, 1981]
SUBPART C—Production of FBI Identification Records in Response to Written Requests by Subjects Thereof

Source:
Order No. 556-73, 38 FR 32806, Nov. 28, 1973, unless otherwise noted.

28 CFR Section 16.30: Purpose and scope.
This subpart contains the regulations of the Federal Bureau of Investigation (FBI) concerning procedures to be followed when the subject of an identification record requests production of that record to review it or to obtain a change, correction, or updating of that record.

Official Citation:
[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

28 CFR Section 16.31: Definition of identification record.
An FBI identification record, often referred to as a “rap sheet,” is a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, includes information taken from fingerprints submitted in connection with federal employment, naturalization, or military service. The identification record includes the name of the agency or institution that submitted the fingerprints to the FBI. If the fingerprints concern a criminal offense, the identification record includes the date of arrest or the date the individual was received by the agency submitting the fingerprints, the arrest charge, and the disposition of the arrest if known to the FBI. All arrest data included in an identification record are obtained from fingerprint submissions, disposition reports, and other reports submitted by agencies having criminal justice responsibilities. Therefore, the FBI Criminal Justice Information Services Division is not the source of the arrest data reflected on an identification record.

Official Citation:
[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

28 CFR Section 16.32: Procedure to obtain an identification record.
The subject of an identification record may obtain a copy thereof by submitting a written request via the U.S. mails directly to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer
Hollow Road, Clarksburg, WV 26306. Such request must be accompanied by satisfactory proof of identity, which shall consist of name, date and place of birth and a set of rolled-inked fingerprint impressions placed upon fingerprint cards or forms commonly utilized for applicant or law enforcement purposes by law enforcement agencies.

**Official Citation:**

---

**28 CFR Section 16.33: Fee for production of identification record.**

Each written request for production of an identification record must be accompanied by a fee of $18 in the form of a certified check or money order, payable to the Treasury of the United States. This fee is established pursuant to the provisions of 31 U.S.C. 9701 and is based upon the clerical time beyond the first quarter hour to be spent in searching for, identifying, and reproducing each identification record requested as specified in § 16.10. Any request for waiver of the fee shall accompany the original request for the identification record and shall include a claim and proof of indigency. Subject to applicable laws, regulations, and directions of the Attorney General of the United States, the Director of the FBI may from time to time determine and establish a revised fee amount to be assessed under this authority. Notice relating to revised fee amounts shall be published in the Federal Register.

**Official Citation:**

---

**28 CFR Section 16.34: Procedure to obtain change, correction or updating of identification records.**

If, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which...

---

Page 290
contributed the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency.

Official Citation:
SUBPART D—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974

Source:
Order No. 2156-98, 63 FR 29600, June 1, 1998, unless otherwise noted.


(a) Purpose and scope.
This subpart contains the rules that the Department of Justice follows under the Privacy Act of 1974, 5 U.S.C. 552a. These rules should be read together with the Privacy Act, which provides additional information about records maintained on individuals. The rules in this subpart apply to all records in systems of records maintained by the Department that are retrieved by an individual's name or personal identifier. They describe the procedures by which individuals may request access to records about themselves, request amendment or correction of those records, and request an accounting of disclosures of those by the Department. In addition, the Department processes all Privacy Act requests for access to records under the Freedom of Information Act (FOIA), 5 U.S.C. 552, following the rules contained in subpart A of this part, which gives requests the benefit of both statutes.

(b) Definitions.
As used in this subpart:

(1) Component
means each separate bureau, office, board, division, commission, service, or administration of the Department of Justice.

(2) Request for access
to a record means a request made under Privacy Act subsection (d)(1).

(3) Request for amendment or correction
of a record means a request made under Privacy Act subsection (d)(2).

(4) Request for an accounting
means a request made under Privacy Act subsection (c)(3).

(5) Requester
means an individual who makes a request for access, a request for amendment or correction, or a request for an accounting under the Privacy Act.
(c) Authority to request records for a law enforcement purpose.
The head of a component or a United States Attorney, or either's designee, is authorized to make written requests under subsection (b)(7) of the Privacy Act for records maintained by other agencies that are necessary to carry out an authorized law enforcement activity.

Official Citation:
[Order No. 2156-98, 63 FR 29600, June 1, 1998; 63 FR 51401, Sept. 25, 1998]

28 CFR Section 16.41: Requests for access to records.

(a) How made and addressed.
You may make a request for access to a Department of Justice record about yourself by appearing in person or by writing directly to the Department component that maintains the record. Your request should be sent or delivered to the component's Privacy Act office at the address listed in appendix I to this part. In most cases, a component's central Privacy Act office is the place to send a Privacy Act request. For records held by a field office of the Federal Bureau of Investigation (FBI) or the Immigration and Naturalization Service (INS), however, you must write directly to that FBI or INS field office address, which can be found in most telephone books or by calling the component's central Privacy Act office. (The functions of each component are summarized in Part o of this title and in the description of the Department and its components in the “United States Government Manual,” which is issued annually and is available in most libraries, as well as for sale from the Government Printing Office's Superintendent of Documents. This manual also can be accessed electronically at the Government Printing Office's World Wide Web site (which can be found at http://www.access.gpo.gov/su_docs). If you cannot determine where within the Department to send your request, you may send it to the FOIA/PA Mail Referral Unit, Justice Management Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001, and that office will forward it to the component(s) it believes most likely to have the records that you seek. For the quickest possible handling, you should mark both your request letter and the envelope “Privacy Act Request.”

(b) Description of records sought.
You must describe the records that you want in enough detail to enable Department personnel to locate the system of records containing them with a reasonable amount of effort. Whenever possible, your request should describe the records sought, the time periods in which you believe they were compiled, and the name or identifying number of each system of records in which you believe they are kept. The Department publishes notices in the Federal Register that describe its components' systems of records. A description of the Department's
systems of records also may be found as part of the “Privacy Act Compilation” published by the National Archives and Records Administration’s Office of the Federal Register. This compilation is available in most large reference and university libraries. This compilation also can be accessed electronically at the Government Printing Office’s World Wide Web site (which can be found at http://www.access.gpo.gov/su_docs).

(c) Agreement to pay fees.
If you make a Privacy Act request for access to records, it shall be considered an agreement by you to pay all applicable fees charged under § 16.49, up to $25.00. The component responsible for responding to your request ordinarily shall confirm this agreement in an acknowledgement letter. When making a request, you may specify a willingness to pay a greater or lesser amount.

(d) Verification of identity.
When you make a request for access to records about yourself, you must verify your identity. You must state your full name, current address, and date and place of birth. You must sign your request and your signature must either be notarized or submitted by you under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the FOIA/PA Mail Referral Unit, Justice Management Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001. In order to help the identification and location of requested records, you may also, at your option, include your social security number.

(e) Verification of guardianship.
When making a request as the parent or guardian of a minor or as the guardian of someone determined by a court to be incompetent, for access to records about that individual, you must establish:

1) The identity of the individual who is the subject of the record, by stating the name, current address, date and place of birth, and, at your option, the social security number of the individual;

2) Your own identity, as required in paragraph (d) of this section;

3) That you are the parent or guardian of that individual, which you may prove by providing a copy of the individual’s birth certificate showing your parentage or by providing a court order establishing your guardianship; and

4) That you are acting on behalf of that individual in making the request.

Official Citation:
[Order No. 2156-98, 63 FR 29600, June 1, 1998; 63 FR 34965, June 26, 1998; 63 FR 51401, Sept. 25, 1998]
28 CFR Section 16.42: Responsibility for responding to requests for access to records.

(a) In general. Except as stated in paragraphs (c), (d), and (e) of this section, the component that first receives a request for access to a record, and has possession of that record, is the component responsible for responding to the request. In determining which records are responsive to a request, a component ordinarily shall include only those records in its possession as of the date the component begins its search for them. If any other date is used, the component shall inform the requester of that date.

(b) Authority to grant or deny requests. The head of a component, or the component head’s designee, is authorized to grant or deny any request for access to a record of that component.

(c) Consultations and referrals. When a component receives a request for access to a record in its possession, it shall determine whether another component, or another agency of the Federal Government, is better able to determine whether the record is exempt from access under the Privacy Act. If the receiving component determines that it is best able to process the record in response to the request, then it shall do so. If the receiving component determines that it is not best able to process the record, then it shall either:

(1) Respond to the request regarding that record, after consulting with the component or agency best able to determine whether the record is exempt from access and with any other component or agency that has a substantial interest in it; or

(2) Refer the responsibility for responding to the request regarding that record to the component best able to determine whether it is exempt from access, or to another agency that originated the record (but only if that agency is subject to the Privacy Act). Ordinarily, the component or agency that originated a record will be presumed to be best able to determine whether it is exempt from access.

(d) Law enforcement information. Whenever a request is made for access to a record containing information that relates to an investigation of a possible violation of law and that was originated by another component or agency, the receiving component shall either refer the responsibility for responding to the request regarding that information to that other component or agency or shall consult with that other component or agency.
(e) Classified information. Whenever a request is made for access to a record containing information that has been classified by or may be appropriate for classification by another component or agency under Executive Order 12958 or any other executive order concerning the classification of records, the receiving component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, should consider the information for classification, or has the primary interest in it, as appropriate. Whenever a record contains information that has been derivatively classified by a component because it contains information classified by another component or agency, the component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the underlying information.

(f) Notice of referral. Whenever a component refers all or any part of the responsibility for responding to a request to another component or agency, it ordinarily shall notify the requester of the referral and inform the requester of the name of each component or agency to which the request has been referred and of the part of the request that has been referred.

(g) Timing of responses to consultations and referrals. All consultations and referrals shall be handled according to the date the Privacy Act access request was initially received by the first component or agency, not any later date.

(h) Agreements regarding consultations and referrals. Components may make agreements with other components or agencies to eliminate the need for consultations or referrals for particular types of records.

Official Citation:

28 CFR Section 16.43: Responses to requests for access to records.

(a) Acknowledgements of requests. On receipt of a request, a component ordinarily shall send an acknowledgement letter to the requester which shall confirm the requester's agreement to pay fees under § 16.41(c) and provide an assigned request number for further reference.

(b) Grants of requests for access.
Once a component makes a determination to grant a request for access in whole or in part, it shall notify the requester in writing. The component shall inform the requester in the notice of any fee charged under § 16.49 and shall disclose records to the requester promptly on payment of any applicable fee. If a request is made in person, the component may disclose records to the requester directly, in a manner not unreasonably disruptive of its operations, on payment of any applicable fee and with a written record made of the grant of the request. If a requester is accompanied by another person, the requester shall be required to authorize in writing any discussion of the records in the presence of the other person.

(c) Adverse determinations of requests for access.
A component making an adverse determination denying a request for access in any respect shall notify the requester of that determination in writing. Adverse determinations, or denials of requests, consist of: A determination to withhold any requested record in whole or in part; a determination that a requested record does not exist or cannot be located; a determination that what has been requested is not a record subject to the Privacy Act; a determination on any disputed fee matter; and a denial of a request for expedited treatment. The notification letter shall be signed by the head of the component, or the component head's designee, and shall include:

(1) The name and title or position of the person responsible for the denial;

(2) A brief statement of the reason(s) for the denial, including any Privacy Act exemption(s) applied by the component in denying the request; and

(3) A statement that the denial may be appealed under § 16.45(a) and a description of the requirements of § 16.45(a).

28 CFR Section 16.44: Classified information.
In processing a request for access to a record containing information that is classified under Executive Order 12958 or any other executive order, the originating component shall review the information to determine whether it should remain classified. Information determined to no longer require classification shall not be withheld from a requester on the basis of Exemption (k)(1) of the Privacy Act. On receipt of any appeal involving classified information, the Office of Information and Privacy shall take appropriate action to ensure compliance with part 17 of this title.
28 CFR Section 16.45: Appeals from denials of requests for access to records.

(a) Appeals.
If you are dissatisfied with a component's response to your request for access to records, you may appeal an adverse determination denying your request in any respect to the Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, DC 20530-0001. You must make your appeal in writing and it must be received by the Office of Information and Privacy within 60 days of the date of the letter denying your request. Your appeal letter may include as much or as little related information as you wish, as long as it clearly identifies the component determination (including the assigned request number, if known) that you are appealing. For the quickest possible handling, you should mark both your appeal letter and the envelope “Privacy Act Appeal.” Unless the Attorney General directs otherwise, a Director of the Office of Information and Privacy will act on behalf of the Attorney General on all appeals under this section, except that:

(1) In the case of an adverse determination by the Deputy Attorney General or the Associate Attorney General, the Attorney General or the Attorney General’s designee will act on the appeal;

(2) An adverse determination by the Attorney General will be the final action of the Department; and

(3) An appeal ordinarily will not be acted on if the request becomes a matter of litigation.

(b) Responses to appeals.
The decision on your appeal will be made in writing. A decision affirming an adverse determination in whole or in part will include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, and will inform you of the Privacy Act provisions for court review of the decision. If the adverse determination is reversed or modified on appeal in whole or in part, you will be notified in a written decision and your request will be reprocessed in accordance with that appeal decision.

(c) When appeal is required.
If you wish to seek review by a court of any adverse determination or denial of a request, you must first appeal it under this section.

28 CFR Section 16.46: Requests for amendment or correction of records.
(a) How made and addressed. Unless the record is not subject to amendment or correction as stated in paragraph (f) of this section, you may make a request for amendment or correction of a Department of Justice record about yourself by writing directly to the Department component that maintains the record, following the procedures in § 16.41. Your request should identify each particular record in question, state the amendment or correction that you want, and state why you believe that the record is not accurate, relevant, timely, or complete. You may submit any documentation that you think would be helpful. If you believe that the same record is in more than one system of records, you should state that and address your request to each component that maintains a system of records containing the record.

(b) Component responses. Within ten working days of receiving your request for amendment or correction of records, a component shall send you a written acknowledgment of its receipt of your request, and it shall promptly notify you whether your request is granted or denied. If the component grants your request in whole or in part, it shall describe the amendment or correction made and shall advise you of your right to obtain a copy of the corrected or amended record, in disclosable form. If the component denies your request in whole or in part, it shall send you a letter signed by the head of the component, or the component head’s designee, that shall state:

(1) The reason(s) for the denial; and

(2) The procedure for appeal of the denial under paragraph (c) of this section, including the name and business address of the official who will act on your appeal.

(c) Appeals. You may appeal a denial of a request for amendment or correction to the Office of Information and Privacy in the same manner as a denial of a request for access to records (see § 16.45) and the same procedures shall be followed. If your appeal is denied, you shall be advised of your right to file a Statement of Disagreement as described in paragraph (d) of this section and of your right under the Privacy Act for court review of the decision.

(d) Statements of Disagreement. If your appeal under this section is denied in whole or in part, you have the right to file a Statement of Disagreement that states your reason(s) for disagreeing with the Department’s denial of your request for amendment or correction. Statements of Disagreement must be concise, must clearly identify each part of any record that is disputed, and should be no longer than one typed page for each fact disputed. Your Statement of Disagreement must be sent to the component involved, which shall place it in the system of records in which the disputed record is maintained and shall mark the disputed record to indicate that a
Statement of Disagreement has been filed and where in the system of records it may be found.

(e) Notification of amendment/correction or disagreement.
Within 30 working days of the amendment or correction of a record, the component that maintains the record shall notify all persons, organizations, or agencies to which it previously disclosed the record, if an accounting of that disclosure was made, that the record has been amended or corrected. If an individual has filed a Statement of Disagreement, the component shall append a copy of it to the disputed record whenever the record is disclosed and may also append a concise statement of its reason(s) for denying the request to amend or correct the record.

(f) Records not subject to amendment or correction.
The following records are not subject to amendment or correction:

(1) Transcripts of testimony given under oath or written statements made under oath;

(2) Transcripts of grand jury proceedings, judicial proceedings, or quasi-judicial proceedings, which are the official record of those proceedings;

(3) Presentence records that originated with the courts; and

(4) Records in systems of records that have been exempted from amendment and correction under Privacy Act, 5 U.S.C. 552a(j) or (k) by notice published in the Federal Register.


(a) How made and addressed.
Except where accountings of disclosures are not required to be kept (as stated in paragraph (b) of this section), you may make a request for an accounting of any disclosure that has been made by the Department to another person, organization, or agency of any record about you. This accounting contains the date, nature, and purpose of each disclosure, as well as the name and address of the person, organization, or agency to which the disclosure was made. Your request for an accounting should identify each particular record in question and should be made by writing directly to the Department component that maintains the record, following the procedures in § 16.41.
(b) Where accountings are not required.
Components are not required to provide accountings to you where they relate to:

(1) Disclosures for which accountings are not required to be kept—in other words, disclosures that are made to employees within the agency and disclosures that are made under the FOIA;

(2) Disclosures made to law enforcement agencies for authorized law enforcement activities in response to written requests from those law enforcement agencies specifying the law enforcement activities for which the disclosures are sought; or

(3) Disclosures made from law enforcement systems of records that have been exempted from accounting requirements.

(c) Appeals.
You may appeal a denial of a request for an accounting to the Office of Information and Privacy in the same manner as a denial of a request for access to records (see § 16.45) and the same procedures will be followed.

Each component will preserve all correspondence pertaining to the requests that it receives under this subpart, as well as copies of all requested records, until disposition or destruction is authorized by title 44 of the United States Code or the National Archives and Records Administration's General Records Schedule 14. Records will not be disposed of while they are the subject of a pending request, appeal, or lawsuit under the Act.

Components shall charge fees for duplication of records under the Privacy Act in the same way in which they charge duplication fees under § 16.11. No search or review fee may be charged for any record unless the record has been exempted from access under Exemptions (j)(2) or (k)(2) of the Privacy Act.

28 CFR Section 16.50: Notice of court-ordered and emergency disclosures.
(a) Court-ordered disclosures.
When a record pertaining to an individual is required to be disclosed by a court order, the component shall make reasonable efforts to provide notice of this to the individual. Notice shall be given within a reasonable time after the component's receipt of the order—except that in a case in which the order is not a matter of public record, the notice shall be given only after the order becomes public. This notice shall be mailed to the individual's last known address and shall contain a copy of the order and a description of the information disclosed. Notice shall not be given if disclosure is made from a criminal law enforcement system of records that has been exempted from the notice requirement.

(b) Emergency disclosures.
Upon disclosing a record pertaining to an individual made under compelling circumstances affecting health or safety, the component shall notify that individual of the disclosure. This notice shall be mailed to the individual's last known address and shall state the nature of the information disclosed; the person, organization, or agency to which it was disclosed; the date of disclosure; and the compelling circumstances justifying the disclosure.

Official Citation:
[Order No. 2156-98, 63 FR 29600, June 1, 1998; 63 FR 51401, Sept. 25, 1998]

(a) Each component shall establish administrative and physical controls to prevent unauthorized access to its systems of records, to prevent unauthorized disclosure of records, and to prevent physical damage to or destruction of records. The stringency of these controls shall correspond to the sensitivity of the records that the controls protect. At a minimum, each component's administrative and physical controls shall ensure that:

(1) Records are protected from public view;

(2) The area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to them;

(3) Records are inaccessible to unauthorized persons outside of business hours; and

(4) Records are not disclosed to unauthorized persons or under unauthorized circumstances in either oral or written form.

(b) Each component shall have procedures that restrict access to records to only those individuals within the Department who must have access to those records.
in order to perform their duties and that prevent inadvertent disclosure of records.

**Official Citation:**
[Order No. 2156-98, 63 FR 29600, June 1, 1998; 63 FR 34965, June 26, 1998]

**28 CFR Section 16.52:** Contracts for the operation of record systems.

Any approved contract for the operation of a record system will contain the standard contract requirements issued by the General Services Administration to ensure compliance with the requirements of the Privacy Act for that record system. The contracting component will be responsible for ensuring that the contractor complies with these contract requirements.

**28 CFR Section 16.53:** Use and collection of social security numbers.

Each component shall ensure that employees authorized to collect information are aware:

(a) That individuals may not be denied any right, benefit, or privilege as a result of refusing to provide their social security numbers, unless the collection is authorized either by a statute or by a regulation issued prior to 1975; and

(b) That individuals requested to provide their social security numbers must be informed of:

   (1) Whether providing social security numbers is mandatory or voluntary;

   (2) Any statutory or regulatory authority that authorizes the collection of social security numbers; and

   (3) The uses that will be made of the numbers.

**28 CFR Section 16.54:** Employee standards of conduct.

Each component will inform its employees of the provisions of the Privacy Act, including the Act’s civil liability and criminal penalty provisions. Unless otherwise permitted by law, an employee of the Department of Justice shall:
(a) Collect from individuals only the information that is relevant and necessary to discharge the responsibilities of the Department;

(b) Collect information about an individual directly from that individual whenever practicable;

(c) Inform each individual from whom information is collected of:

   (1) The legal authority to collect the information and whether providing it is mandatory or voluntary;

   (2) The principal purpose for which the Department intends to use the information;

   (3) The routine uses the Department may make of the information; and

   (4) The effects on the individual, if any, of not providing the information;

(d) Ensure that the component maintains no system of records without public notice and that it notifies appropriate Department officials of the existence or development of any system of records that is not the subject of a current or planned public notice;

(e) Maintain all records that are used by the Department in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination;

(f) Except as to disclosures made to an agency or made under the FOIA, make reasonable efforts, prior to disseminating any record about an individual, to ensure that the record is accurate, relevant, timely, and complete;

(g) Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity;

(h) When required by the Act, maintain an accounting in the specified form of all disclosures of records by the Department to persons, organizations, or agencies;

   (i) Maintain and use records with care to prevent the unauthorized or inadvertent disclosure of a record to anyone; and

(j) Notify the appropriate Department official of any record that contains information that the Privacy Act does not permit the Department to maintain.
28 CFR Section 16.55: Other rights and services.

Nothing in this subpart shall be construed to entitle any person, as of right, to any service or to the disclosure of any record to which such person is not entitled under the Privacy Act.

SUBPART E—Exemption of Records Systems Under the Privacy Act

Source:
Order No. 645-76, 41 FR 12640, Mar. 26, 1976, unless otherwise noted.


(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e)(1), (2) and (3), (e)(4) (G) and (H), (e)(5); and (g):


These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest on the part of the Department of Justice as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.
(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official Federal investigations. Individual access to these records might compromise ongoing investigations, reveal confidential informants or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations of duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsections (e)(4) (G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (g) because this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

Official Citation: [Order No. 31-85, 51 FR 751, Jan. 8, 1986]

(a) The following systems of records and exempt from 5 U.S.C. 552a(d)(1) and (e)(1):


These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

1. From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a Presidential appointee or Department attorney position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department of Justice. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

2. From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate for a position which assists in determining whether that candidate should be nominated for appointment.

(c) The following systems of records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (2), (3) and (5); and (g):


(d) In addition, the Drug Enforcement Task Force Evaluation and Reporting System is exempt from 5 U.S.C. 552a(e)(4)(G) and (H). The exemptions for the Drug Enforcement Task Force Evaluation and Reporting System apply only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). The exemptions for the General Files System apply only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(e) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her could reveal investigative interest on the part of the Department of Justice, as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel. Further, making available to a record subject the accounting of disclosures could reveal the identity of a confidential source. In addition, release of an accounting of disclosures from the General Files System may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security.

(2) From subsection (c)(4) because these systems are exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in these systems relate to official Federal investigations. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. In addition, release of records from the General Files System may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security. Amendment of the records in either of these systems would interfere with ongoing law enforcement proceedings and impose an impossible administrative burden by requiring law enforcement investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or
introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede any investigative process, whether civil or criminal, if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and may therefore be able to avoid detection, apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsections (e)(4) (G) and (H) because no access to these records is available under subsection (d) of the Privacy Act. (This exemption applies only to the Drug Enforcement Task Force Evaluation and Reporting System.)

(8) From subsection (g) because these systems of records are exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

Official Citation:
[Order No. 57-91, 56 FR 58305, Nov. 19, 1991]


(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e)(1), (2), (3) and (5); and (g):


These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her could reveal investigative interest on the part of the Department of Justice, as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel. Further, making available to a record subject the accounting of disclosures could reveal the identity of a confidential source. In addition, release of an accounting of disclosures may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official Federal investigations. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. In addition, release of these records may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security. Amendment of the records in this system would interfere with ongoing law enforcement proceedings and impose an impossible administrative burden by requiring law enforcement investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede any investigative process, whether civil or criminal, if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and may therefore be able to avoid detection, apprehension, or legal obligations or duties.
(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsection (g) because this system of records is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act.

**Official Citation:**
[Order No. 57-91, 56 FR 58305, Nov. 19, 1991]

---

**28 CFR Section 16.73: Exemption of Office of Legal Policy System—limited access.**

(a) The following system of records is exempt from 5 U.S.C 552a (d)(1), (2), (3) and (4); (e)(1) and (2), (e)(4)(G) and (H), (e)(5); and (g):

(1) Freedom of Information and Privacy Appeals Index (JUSTICE/OLP-001).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2) and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (d)(1), (2), (3), and (4) to the extent that information in this record system relates to official Federal investigations and matters of law enforcement. Individual access to these records might compromise ongoing investigations, reveal confidential informants or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(2) From subsections (e)(1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness, and completeness of all information obtained.
(3) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations or duties.

(4) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(5) From subsection (g) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(c) The following system of records is exempt from 5 U.S.C. 552a(d)(1) and (e)(1):


These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contracted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a judgeship. Access could reveal the identity of the source of the information and constitute a breach of the promised confidentiality on the part of the Department. Such breaches ultimately would restrict the free flow of information vital to the determination of a candidate's qualifications and suitability.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may seem irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate which assists in determining whether that candidate should be nominated for appointment.

(e) The following system of records is exempt from U.S.C. 552a(c) (3) and (4); (d); (e)(1), (2) and (3), (e)(4)(G) and (H) (e)(5); and (g):
(1) General Files System of the Office of Legal Policy (JUSTICE/OLP-003).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest on the part of the Department as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official Federal investigations. Individual access to these records might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information since it may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigation process if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsections (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations and duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

Page 313
(7) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (g) because this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d); (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5); and (g):

(1) Declassification Review System (JUSTICE/OLP-004).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552(j)(2), (k)(1), (k)(2), and (k)(5).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest on the part of the Department of Justice as well as the recipient agency. This would permit record subjects to impede the investigation e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) to the extent that information in this record system relates to official Federal investigations and matters of law enforcement and/or is properly classified pursuant to E.O. 12356. Individual access to these records might compromise ongoing investigations, reveal confidential sources or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation, or jeopardize national security or foreign policy interests. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information which may aid in establishing patterns.
of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness, and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsections (e)(4) (G) and (H), and (g) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

Official Citation:


(a) The following system of records is exempted from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2) and (5): Foreign Intelligence and Counterintelligence Records System (JUSTICE/NSD-001). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) Subsection (c)(3).

To provide the target of a surveillance or collection activity with the disclosure accounting records concerning him or her would hinder authorized United States intelligence activities by informing that individual of the existence, nature, or
scope of information that is properly classified pursuant to Executive Order 12958, as amended, and thereby cause damage to the national security.

(2) Subsection (c)(4).
This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) Subsection (d)(1).
Disclosure of foreign intelligence and counterintelligence information would interfere with collection activities, reveal the identity of confidential sources, and cause damage to the national security of the United States. To ensure unhampered and effective collection and analysis of foreign intelligence and counterintelligence information, disclosure must be precluded.

(4) Subsection (d)(2).
Amendment of the records would interfere with ongoing intelligence activities thereby causing damage to the national security.

(5) Subsections (d)(3) and (4).
These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) Subsection (e)(1).
It is often impossible to determine in advance if intelligence records contained in this system are relevant and necessary, but, in the interests of national security, it is necessary to retain this information to aid in establishing patterns of activity and provide intelligence leads.

(7) Subsection (e)(2).
Although this office does not conduct investigations, the collection efforts of agencies that supply information to this office would be thwarted if the agencies were required to collect information with the subject's knowledge.
To inform individuals as required by this subsection could reveal the existence of collection activity and compromise national security. For example, a target could, once made aware that collection activity exists, alter his or her manner of engaging in intelligence or terrorist activities in order to avoid detection.

(9) Subsections (e)(4)(G), (H) and (I), and (f).

These subsections are inapplicable to the extent that this system is exempt from the access provisions of subsection (d).

(10) Subsection (e)(5).

It is often impossible to determine in advance if intelligence records contained in this system are accurate, relevant, timely and complete, but, in the interests of national security, it is necessary to retain this information to aid in establishing patterns of activity and providing intelligence leads.

(11) Subsection (e)(8).

Serving notice could give persons sufficient warning to evade intelligence collection and anti-terrorism efforts.

(12) Subsections (g) and (h).

These subsections are inapplicable to the extent that this system is exempt from other specific subsections of the Privacy Act.

Official Citation:
[Order No. 023-2007, 72 FR 44382, Aug. 8, 2007]


(a) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2), (3), (5), and (8), and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) of 5 U.S.C. 552a:

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the Office of the Inspector General (OIG).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation, and reveal investigative interest by not only the OIG, but also by the recipient agency. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation, release could result in the destruction of documentary evidence, improper influencing of witnesses, endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel, the fabrication of testimony, flight of the subject from the area, and other activities that could impede or compromise the investigation. In addition, accounting for each disclosure could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel, and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information
that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIG for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIG may obtain information concerning actual or potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIG should retain this information, as it may aid in establishing patterns of criminal activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation, information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may relate also to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(5) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject’s illegal acts, violations of rules of conduct, or any other misconduct must be obtained from other sources.
(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

(6) From subsection (e)(3) because the application of this provision would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5) because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Material which may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance as an investigation progresses. The restrictions of this provision could interfere with the preparation of a complete investigative report, and thereby impede effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2) and (k)(1) and (k)(2) of the Privacy Act.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).


This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to official Federal investigations and law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by the Office of the Inspector General (OIG).

(d) Exemption from subsection (d) is justified for the following reasons:
(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(2) [Reserved]

**Official Citation:**
[Order No. 63-92, 57 FR 8263, Mar. 9, 1992, as amended by Order No. 64-92, 57 FR 8263, Mar. 9, 1992]

28 CFR Section 16.76: Exemption of Justice Management Division.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) Controlled Substances Act Nonpublic Records (JUSTICE/JMD-002).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemption from subsection (d) is justified for the following reasons:

(1) Access to and use of the nonpublic records maintained in this system are restricted by law. Section 3607(b) of Title 18 U.S.C. (enacted as part of the Sentencing Reform Act of 1984, Pub. L. 98-473, Chapter II) provides that the sole
purpose of these records shall be for use by the courts in determining whether a person found guilty of violating section 404 of the Controlled Substances Act qualifies:

(i) For the disposition available under 18 U.S.C. 3607(a) to persons with no prior conviction under a Federal or State law relating to controlled substances, or

(ii) For an order, under 18 U.S.C. 3607(c), expunging all official records (except the nonpublic records to be retained by the Department of Justice) of the arrest and any subsequent criminal proceedings relating to the offense.

(2) Information in this system consists of arrest records, including those of co-defendants. The records include reports of informants and investigations. Therefore, access could disclose investigative techniques, reveal the identity of confidential sources, and invade the privacy of third parties.

(c) The following system of records is exempted from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g): Federal Bureau of Investigation Whistleblower Case Files (Justice/JMD-023). These exemptions apply only to the extent that information in a record contained within this system is subject to exemptions pursuant to 5 U.S.C. 552a(j)(2) and (k).

(d) Exemption from the particular subsections is justified for the following reasons:

(1) Subsection (c)(3).

To provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) Subsection (c)(4).

This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) Subsection (d)(1).
Information within this record system could relate to official federal investigations and matters of law enforcement. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Disclosure may also reveal information relating to actual or potential law enforcement investigations. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) Subsection (d)(2).

Amendment of these records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) Subsections (d)(3) and (4).

These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) Subsection (e)(1).

It is often impossible to determine in advance if investigatory information contained in this system is accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) Subsection (e)(2).

To collect information from the subject individual could serve to notify the subject individual that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) Subsection (e)(3).

To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) Subsection (e)(5).
It is often impossible to determine in advance if investigatory information contained in this system is accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) Subsection (e)(8).

To serve notice could give persons sufficient warning to evade investigative efforts.

(11) Subsection (g).

This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:


(a) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4); (d); (e)(1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8); (f) and (g):

(1) U.S. Trustee Program Case Referral System, JUSTICE/UST-004.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the nature of that investigation. This would permit record subjects to
impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) since an exemption being claimed for subsection (d) makes this subsection inapplicable.

(3) From subsection (d) because access to the records contained in this system might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interest of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness, and completeness of all information obtained.

(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement because the subject of the investigation would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it would compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7) From subsections (e)(4) (G) and (H) because this system of records is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k).

(8) From subsection (e)(8) because the individual notice requirement of this subsection could present a serious impediment to law enforcement in that this could interfere with the U.S. Attorney's ability to issue subpoenas.
(9) From subsections (f) and (g) because this system has been exempted from the access provisions of subsection (d).

**Official Citation:**
[Order No. 1-87, 52 FR 3631, Feb. 5, 1987]

---

**28 CFR Section 16.78: Exemption of the Special Counsel for Immigration-Related, Unfair Employment Practices Systems.**

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (d).

(1) Central Index File and Associated Records, JUSTICE/OSC-001.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the nature of that investigation. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries.

(2) From subsection (d) because access to the records might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation.

**Official Citation:**
[Order No. 10-88, 53 FR 7735, Mar. 10, 1988]

---

**28 CFR Section 16.79: Exemption of Pardon Attorney System.**

(a) The following system of records is exempt from 5 U.S.C. 552a, subsections (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), and (e)(5): Executive Clemency Case Files/Executive Clemency Tracking System (JUSTICE/OPA-001). These exemptions apply only to the extent that information in this system of records is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).
(b) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because:

   (i) The purpose of the creation and maintenance of the Executive Clemency Case Files/Executive Clemency Tracking System (JUSTICE/OPA-001) is to enable the Justice Department to prepare reports and recommendations to the President for his ultimate decisions on clemency matters, which are committed to exclusive discretion of the President pursuant to Article II, Section 2, Clause 1 of the Constitution.

   (ii) Release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the requester to obtain valuable information concerning the nature and scope of a clemency investigation, invade the right of candid and confidential communications among officials concerned with making recommendations to the President in clemency matters, and disclose the identity of persons who furnished information to the Government under an express or implied promise that their identities would be held in confidence.

(2) From subsection (c)(4) because the exemption from subsections (d)(1), (d)(2), (d)(3), and (d)(4) will make notification of disputes inapplicable.

(3) From subsections (d)(1), (d)(2), (d)(3), and (d)(4) is justified for the reasons stated in paragraph (b)(1) of this section.

(4) From subsection (e)(5) is justified for the reasons stated in paragraph (b)(1) of this section.

**Official Citation:**

---

**28 CFR Section 16.80:** Exemption of Office of Professional Responsibility System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f) and (g):

(1) Office of Professional Responsibility Record Index (JUSTICE/OPR-001).
These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of the disclosure accounting would enable the subject of an investigation to gain information concerning the existence, nature and scope of the investigation and seriously hamper law enforcement efforts.

(2) From subsections (c)(4), (d), (e)(4)(G) and (H), (f) and (g) because these provisions concern individual access to records and such access might compromise ongoing investigations, reveal confidential informants and constitute unwarranted invasions of the personal privacy of third persons who provide information in connection with a particular investigation.

(3) From subsections (e)(1) and (5) because the collection of information during an investigation necessarily involves material pertaining to other persons or events which is appropriate in a thorough investigation, even though portions thereof are not ultimately connected to the person or event subject to the final action or recommendation of the Office of Professional Responsibility.

(4) From subsection (e)(2) because collecting the information from the subject would thwart the investigation by placing the subject on notice of the investigation.

(5) From subsections (e)(3) and (e)(8) because disclosure and notice would provide the subject with substantial information which could impede or compromise the investigation. For example, an investigatory subject occupying a supervisory position could, once made aware that a misconduct investigation was ongoing, put undue pressure on subordinates so as to preclude their cooperation with investigators.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).

(1) Freedom of Information/Privacy Act (FOI/PA) Records (JUSTICE/OPR-002).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigations and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by OPR.
(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an enormous administrative burden by requiring investigations to be continuously reinvestigated.

Official Citation:
[Order No. 58-81, 46 FR 3509, Jan. 15, 1981, as amended by Order No. 159-99, 64 FR 17977, Apr. 13, 1999]


(a) The following systems of records are exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Citizen Complaint Files (JUSTICE/USA-003).

(2) Civil Case Files (JUSTICE/USA-005).

(3) Consumer Complaints (JUSTICE/USA-006).

(4) Criminal Case Files (JUSTICE/USA-007).
(5) Kline-District of Columbia and Maryland-Stock and Land Fraud Interrelationship Filing System (JUSTICE/USA-009).

(6) Major Crimes Division Investigative Files (JUSTICE/USA-010).

(7) Prosecutor’s Management Information System (PROMIS) (JUSTICE/USA-011).

(8) United States Attorney, District of Columbia Superior Court Division, Criminal Files (JUSTICE/USA-013).

(9) Pre-trial Diversion Program Files (JUSTICE/USA-014).

These exemptions apply to the extent that information in these systems is subject to exemption pursuant to U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for these systems, would permit the subject of a criminal investigation and/or civil case or matter under investigation, litigation, regulatory or administrative review or action, to obtain valuable information concerning the nature of that investigation, case or matter and present a serious impediment to law enforcement or civil legal activities.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in these systems would inform the subject of criminal investigation and/or civil investigation, matter or case of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection, apprehension or legal obligations, and present a serious impediment to law enforcement and other civil remedies.

(4) From subsection (e)(1) because in the course of criminal investigations and/or civil investigations, cases or matters, the U.S. Attorneys often obtain information concerning the violation of laws or civil obligations other than those relating to an active case or matter. In the interests of effective law enforcement and civil litigation, it is necessary that the U.S. Attorneys retain this information since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought within the U.S. Attorneys’ offices.
(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection, apprehension or legal obligations and duties.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because these systems of records are exempt from individual access pursuant to subsections (j) and (k) of the Privacy Act of 1974.

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the United States Attorneys' ability to issue subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (f) because these systems of records have been exempted from the access provisions of subsection (d).

(11) From subsection (g) because these systems of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(c) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

Page 331
(1) Freedom of Information Act/Privacy Act Files (JUSTICE/USA-008)

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(d) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation and/or civil case or matter under investigation, in litigation, or under regulatory or administrative review or action to obtain valuable information concerning the nature of that investigation, case or matter, and present a serious impediment to law enforcement or civil legal activities.

(2) From subsection (c)(4) because an exemption is being claimed for subsection (d) of the Act (Access to Records), rendering this subsection inapplicable to the extent that this system of records is exempted from subsection (d).

(3) From subsection (d) because access to the records contained in these systems would inform the subject of a criminal or civil investigation, matter or case of the existence of such, and provide the subject with information that might enable him to avoid detection, apprehension or legal obligations, and present a serious impediment to law enforcement and other civil remedies. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because in the course of criminal investigations and/or civil investigations, cases or matters, the U.S. Attorneys often obtain information concerning the violation of laws or civil obligations other than those relating to an active case or matter. In the interests of effective law enforcement and civil litigation, it is necessary that the U.S. Attorneys retain this information since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought within the U.S. Attorneys' offices.

(5) From subsection (e)(2) because to collect information to the greatest extent possible from the subject individual of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations and duties.
(6) From subsection (e)(3) because to provide individuals supplying information with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information, and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because this system of records is exempt from the individual access provisions of subsection (d) and the rules provisions of subsection (f).

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would inhibit the ability of trained investigator and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the U.S. Attorneys' ability to issue subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (f) because this system has been exempted from the individual access provisions of subsection (d).

(11) From subsection (g) because the records in this system are generally compiled for law enforcement purposes and are exempt from the access provisions of subsections (d) and (f), rendering subsection (g) inapplicable.

(e) The following systems of records are exempt from 5 U.S.C. 552a(d)(1) and (e)(1):

(1) Assistant U.S. Attorneys Applicant Records System (JUSTICE/USA-016).

(2) Appointed Assistant U.S. Attorneys Personnel System (JUSTICE/USA-017).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).
(f) Exemptions from the particular subsections are justified for the following reasons:

1. From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for an Assistant U.S. Attorney position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department of Justice. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

2. From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate for a position which assists in determining whether that candidate should be nominated for appointment.

(g) The Giglio Impeachment Files (JUSTICE/USA-018) system of records is exempt from 5 U.S.C. 552a subsections (c)(4), (e)(2), (e)(5), and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), and exempt from subsections (c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f), pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(h) Exemptions from the particular subsections are justified for the following reasons:

1. From subsection (c)(3); because an exemption is being claimed for subsection (d), this subsection will not be applicable.

2. From subsection (c)(4); because an exemption is being claimed for subsection (d), this subsection will not be applicable.

3. From subsection (d); because access to the records contained in these systems is not necessary or may impede an ongoing investigation. Most information in the records is derivative from the subject's employing agency files, and individual access will be through the employing agency's files. Additionally, other information in the records may be related to allegations against an agent or witness that are currently being investigated. Providing access to this information would impede the ongoing investigation.
(4) From subsection (e)(1); because in the interest of effective law enforcement and criminal prosecution, Giglio records will be retained because they could later be relevant in a different case; however, this relevance cannot be determined in advance.

(5) From subsection (e)(2); because the nature of the records in this system, which are used to impeach or demonstrate bias of a witness, requires that the information be collected from others.

(6) From subsections (e)(4)(G) and (H); because this system of records is exempt from individual access pursuant to subsections (j) and (k) of the Privacy Act of 1974.

(7) From subsection (e)(5); because the information in these records is not being used to make a determination about the subject of the records. According to constitutional principles of fairness articulated by the Supreme Court in United States v. Giglio, the records are required to be disclosed to criminal defendants to ensure fairness of criminal proceedings.

(8) From subsection (f); because records in this system have been exempted from the access provisions of subsection (d).

(9) From subsection (g); because records in this system are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(i) Consistent with the legislative purpose of the Privacy Act of 1974, the Executive Office for United States Attorneys will grant access to nonexempt material in records which are maintained by the U.S. Attorneys. Disclosure will be governed by the Department's Privacy regulations, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal, civil or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

Official Citation:
28 CFR Section 16.82: Exemption of the National Drug Intelligence Center Data Base—limited access.

(a) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4); (d); (e)(1), (2), and (3); (e)(4)(I); (e) (5) and (8); and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) and (e)(4)(I) of 5 U.S.C. 552a:

(1) National Drug Intelligence Center Data Base (JUSTICE/NDIC-001).

(2) [Reserved]

(b) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the National Drug Intelligence Center (NDIC). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) for the same reasons that the system is exempted from the provisions of subsection (d).

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsection (j)(2) of the Privacy Act.

(3) From subsection (d) because disclosure to the subject could alert the subject of an investigation pertaining to narcotic trafficking or related activity of the fact and nature of the investigation, and/or of the investigative interest of NDIC and other intelligence or law enforcement agencies (including those responsible for civil proceedings related to laws against drug trafficking); lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life and safety of law enforcement personnel, confidential informants, witnesses, and potential
crime victims. Finally, access to records could result in the release of properly classified information that could compromise the national defense or foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because, in the course of its acquisition, collation, and analysis of information, NDIC will need to retain information not immediately shown to be relevant to counterdrug law enforcement to establish patterns of activity and to assist other agencies charged with the enforcement of laws and regulations regarding drug trafficking and charged with the acquisition of intelligence related to international aspects of drug trafficking. This consideration applies equally to information acquired from, or collated or analyzed for, both law enforcement agencies and agencies of the U.S. foreign intelligence community.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to law enforcement in that it would put the subject of an investigation, study or analysis on notice of the fact of such investigation, study, or analysis, thereby permitting the subject to engage in conduct intended to frustrate the activity; because, in some circumstances, the subject of an investigation may not be required to provide to investigators certain information; and because thorough analysis and investigation may require seeking information from a number of different sources.

(6) From subsection (e)(3) (to the extent applicable) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation and reveal the identity of confidential informants and endanger their lives and safety.

(7) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than have been published in the Federal Register. Should the subsection be so interpreted, exemption from this provision is necessary to protect the confidentiality of the sources of criminal and other law enforcement information and to protect the privacy and physical safety of witnesses and informants. Furthermore, greater specificity concerning the sources of properly classified records could compromise national defense or foreign policy.
(8) From subsection (e)(5) because the acquisition, collation, and analysis of information for law enforcement purposes does not permit advance determination whether such information is accurate or relevant, nor can such information be limited to that which is complete or apparently timely. Information of this type often requires further analysis and investigation to develop into a comprehensive whole that which is otherwise incomplete or even fragmentary. Moreover, its accuracy is continually subject to analysis and review, and, upon careful examination, seemingly irrelevant or untimely information may acquire added significance as additional information brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in collating and analyzing information and would impede the development of criminal intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement by revealing investigative techniques, procedures, or evidence.

(10) From subsection (g) to the extent that the system is exempt from subsection (d).

Official Citation:
[Order No. 78-93, 58 FR 41038, Aug. 2, 1993]

28 CFR Section 16.83: Exemption of the Executive Office for Immigration Review System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) The Executive Office for Immigration Review’s Records and Management Information System (JUSTICE/EOIR-001).

This exemption applies only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1) and (2).

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsection (d) because access to information which has been properly classified pursuant to an Executive Order could have an adverse effect on the national security. In addition, from subsection (d) because unauthorized access to certain investigatory material could compromise ongoing or potential
investigations; reveal the identity of confidential informants; or constitute unwarranted invasions of the personal privacy of third parties.

(2) From subsection (d) (2), (3), and (4) because the record of proceeding constitutes an official record which includes transcripts of quasi-judicial administrative proceedings, investigatory materials, evidentiary materials such as exhibits, decisional memoranda, and other case-related papers. Administrative due process could not be achieved by the ex parte “correction” of such materials by the individual who is the subject thereof.

(c) The following system of records is exempted form 5 U.S.C. 552a(d).

(1) Practitioner Compliant/Disciplinary Files (JUSTICE/EOIR 003). This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official federal investigations and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law or regulatory enforcement process, the applicable exemption may be waived by the Executive Office for Immigration Review.

(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of the investigation of an actual or potential criminal, civil, or regulatory violation or the existence of that investigation; of the nature and scope of the information and evidence obtained as to the subject’s activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law and regulatory enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an enormous administrative burden by requiring investigations to be continuously reinvestigated.
Official Citation:
[Order No. 18-86, 51 FR 32305, Sept. 11, 1986, as amended by Order No. 180-99, 64 FR 61787, Nov. 15, 1999]

28 CFR Section 16.84: Exemption of Immigration Appeals System.

(a) The following system of records is exempt from 5 U.S.C. 552a(d) (2), (3) and (4):

(1) Decisions of the Board of Immigration Appeals (JUSTICE/BIA-001).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (d) (2), (3) and (4) because the decisions reflected constitute official records of opinions rendered in quasi-judicial proceedings. Administrative due process could not be achieved by the ex parte “correction” of such opinions by the subject of the opinion.


(a) The following systems of records are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e)(8), (f) and (g):

(1) Docket Scheduling and Control System (JUSTICE/PRC-001).

(2) Inmate and Supervision Files System (JUSTICE/PRC-003).

(3) Labor and Pension Case, Legal File, and General Correspondence System (JUSTICE/PRC-004).


(5) Workload Record, Decision Result, and Annual Report System (JUSTICE/PRC-007).

Page 340
These exemptions apply only to the extent that information in these systems is subject to exemptions pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because revealing disclosure of accountings to inmates and persons on supervision could compromise legitimate law enforcement activities and U.S. Parole Commission responsibilities.

(2) From subsection (c)(4) because the exemption from subsection (d) will make notification of disputes inapplicable.

(3) From subsection (d) because this is essential to protect internal processes by which Commission personnel are able to formulate decisions and policies with regard to federal prisoners and persons under supervision, to prevent disclosures of information to federal inmates or persons on supervision that would jeopardize legitimate correctional interests of security, custody, supervision, or rehabilitation, to permit receipt of relevant information from other federal agencies, state and local law enforcement agencies, and federal and state probation and judicial offices, to allow private citizens to express freely their opinions for or against parole, to allow relevant criminal history type information of co-defendants to be kept in files, to allow medical, psychiatric and sociological material to be available to professional staff, and to allow a candid process of fact selection, opinion formulation, evaluation and recommendation to be continued by professional staff. The legal files contain case development material and, in addition to other reasons, should be exempt under the attorney-client privilege. Each labor or pension applicant has had served upon him the material in his file which he did not prepare and may see his own file at any time.

(4) From subsection (e)(2) because primary collection of information directly from federal inmates or persons on supervision about criminal sentence, criminal records, institutional performance, readiness for release from custody, or need to be returned to custody is highly impractical and inappropriate.

(5) From subsection (e)(3) because application of this provision to the operations and collection of information by the Commission which is primarily from sources other than the individual, is inappropriate.

(6) From subsections (e)(4) (G) and (H) because exemption from the access provisions of (d) makes publication of agency procedures under (d) inapplicable.
(7) From subsection (e)(8) because the nature of the Commission's activities renders notice of compliance with compulsory legal process impractical.

(8) From subsection (f) because exemption from the provisions of subsection (d) will render compliance with provisions of this subsection inapplicable.

(9) From subsection (g) because exemption from the provisions of subsection (d) will render the provisions on suits to enforce (d) inapplicable.

(c) Consistent with the legislative purpose of the Privacy Act of 1974 the U.S. Parole Commission will initiate a procedure whereby present and former prisoners and parolees may obtain copies of material in files relating to them that are maintained by the U.S. Parole Commission. Disclosure of the contents will be affected by providing copies of documents to requesters through the mails. Disclosure will be made to the same extent as would be made under the substantive exemptions of the Parole Commission and Reorganization Act of 1976 (18 U.S.C. 4208) and Rule 32 of the Federal Rules of Criminal Procedure. The procedure relating to disclosure of documents may be changed generally in the interest of improving the Commission's system of disclosure or when required by pending or future decisions and directions of the Department of Justice.

Official Citation:

28 CFR Section 16.88: Exemption of Antitrust Division Systems—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(4) (G) and (H), and (f):


These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(b) Exemption from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3) because information in this system is maintained in aid of ongoing antitrust enforcement investigations and proceedings. The release of the accounting of disclosures made under subsection (b) of the Act would permit the subject of an investigation of an actual or potential criminal or civil violation to determine whether he is the subject of an investigation. Disclosure of the accounting would therefore present a serious impediment to antitrust law enforcement efforts.

(2) From subsection (d) because access to the information retrievable from this system and compiled for law enforcement purposes could result in the premature disclosure of the identity of the subject of an investigation of an actual or potential criminal or civil violation and information concerning the nature of that investigation. This information could enable the subject to avoid detection or apprehension. This would present a serious impediment to effective law enforcement since the subject could hinder or prevent the successful completion of the investigation. Further, confidential business and financial information, the identities of confidential sources of information, third party privacy information, and statutorily confidential information such as grand jury information must be protected from disclosure.

(3) From subsections (e)(4)(G) and (H), and (f) because this system is exempt from the individual access provisions of subsection (d).

(c) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(4)(G) and (H), and (f):

(1) Freedom of Information/Privacy—Requester/Subject Index File (JUSTICE/ATR-008).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(d) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the accounting of disclosures made under subsection (b) of the Act would permit the subject of an investigation of an actual or potential criminal or civil violation to determine whether he is the subject of an investigation. Disclosure of会计 would therefore present a serious impediment to antitrust law enforcement efforts.

(2) From subsection (d) because access to information in this system could result in the premature disclosure of the identity of the subject of an investigation
of an actual or potential criminal or civil violation and information concerning
the nature of the investigation. This information could enable the subject to avoid
detection or apprehension. This would present a serious impediment to effective
law enforcement since the subject could hinder or prevent the successful
completion of the investigation. Further, confidential business and financial
information, the identities of confidential sources of information, third party
privacy information, and statutorily confidential information such as grand jury
information must be protected from disclosure.

(3) From subsections (e)(4)(G) and (H), and (f) because this system is
exempt from the individual access provisions of subsection (d).

Official Citation:
[Order No. 2-86, 51 FR 884, Jan. 9, 1986]

28 CFR Section 16.89: Exemption of Civil Division Systems—
limited access.

(a) The following systems of records are exempted pursuant to 5 U.S.C. 552a(j)(2)
from subsections (c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4) (G) and (H),
(e)(5), (e)(8), and (g); in addition, the following systems of records are exempted
pursuant to 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1),
(e)(4) (G) and (H):

(1) Civil Division Case File System, JUSTICE/CIV-001.


These exemptions apply only to the extent that information in these
systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) Only that information which relates to the investigation, prosecution, or
defense of actual or potential criminal or civil litigation, or which has been
properly classified in the interest of national defense and foreign policy is
exempted for the reasons set forth from the following subsections:

(1) Subsection (c)(3).
To provide the subject of a criminal or civil matter or case under investigation
with an accounting of disclosures of records concerning him or her would inform
that individual (and others to whom the subject might disclose the records) of the
existence, nature, or scope of that investigation and thereby seriously impede law
enforcement efforts by permitting the record subject and others to avoid criminal
penalties and civil remedies.
(2) Subsections (c)(4), (e)(4) (G) and (H), and (g).
These provisions are inapplicable to the extent that these systems of records are exempted from subsection (d).

(3) Subsection (d).
To the extent that information contained in these systems has been properly classified, relates to the investigation and/or prosecution of grand jury, civil fraud, and other law enforcement matters, disclosure could compromise matters which should be kept secret in the interest of national security or foreign policy; compromise confidential investigations or proceedings; hamper sensitive civil or criminal investigations; impede affirmative enforcement actions based upon alleged violations of regulations or of civil or criminal laws; reveal the identity of confidential sources; and result in unwarranted invasions of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) Subsection (e)(1).
In the course of criminal or civil investigations, cases, or matters, the Civil Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.

(5) Subsection (e)(2).
To collect information from the subject of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject (and others to whom the subject might be in contact) would be informed of the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) Subsection (e)(3).
To comply with this requirement during the course of a criminal investigation or prosecution could jeopardize the investigation by disclosing the existence of a confidential investigation, revealing the identity of witnesses or confidential informants, or impeding the information gathering process.

(7) Subsection (e)(5).
In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of
law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(8) Subsection (e)(8).
To serve notice would give persons sufficient warning to evade law enforcement efforts.

c) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1) and (e)(5); in addition, this system is also exempted pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d), and (e)(1).


These exemptions apply only to the extent that information in this system of records is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

d) Only that information compiled for criminal or civil law enforcement purposes is exempted for the reasons set forth from the following subsections:

(1) Subsections (c)(3).
This system occasionally contains investigatory material based on complaints of actual or alleged criminal or civil violations. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him/her would inform that individual of the existence, nature, or scope of that investigation, and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties and civil remedies.

(2) Subsections (c)(4).
This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) Subsection (d).
Disclosure of information relating to the investigation of complaints of alleged violation of criminal or civil law could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) Subsection (e)(1).
In the course of criminal or civil investigations, cases, or matters, the Civil Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.

(5) Subsection (e)(5).
In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(e) The following system of records is exempt pursuant to 5 U.S.C. 552a (j)(2) and (k)(2) from subsection (d):

Source: Congressional and Citizen Correspondence File, JUSTICE/CIV-007.

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C 552a (j)(2) and (k)(2).

(f) Only that portion of the Congressional and Citizen Correspondence File maintained by the Communications Office which consists of criminal or civil investigatory information is exempted for the reasons set forth from the following subsection:

(1) Subsection (d).
Disclosure of investigatory information would jeopardize the integrity of the investigative process, disclose the identity of individuals who furnished information to the government under an express or implied promise that their identities would be held in confidence, and result in an unwarranted invasion of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

Official Citation:
[Order No. 27-88, 54 FR 113, Jan. 4, 1989]

(a) The following system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j) and (k): Central Civil Rights Division Index File and Associated Records (JUSTICE/CRT-001). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) Subsection (c)(3).
To provide the subject of a criminal, civil, or administrative matter or case under investigation with an accounting of disclosures of records concerning him or her could inform that individual of the existence, nature, or scope of an actual or potential criminal or civil violation to gain valuable information concerning the nature and scope of the investigation, to determine whether he or she is the subject of the investigation, and seriously impede law enforcement efforts by permitting the record subject and other persons to whom he or she might disclose the records to avoid criminal penalties, civil remedies, or administrative measures.

(2) Subsection (c)(4).
This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) Subsection (d)(1).
Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Disclosure of classified national security information would cause damage to the national security of the United States. In addition, these records may be subject to protective orders entered by federal courts to protect their confidentiality. Further, many of the records contained in this system are copies of documents which are the property of state agencies and were obtained under express or implied promises to strictly protect their confidentiality.

(4) Subsection (d)(2).
Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) Subsection (d)(3) and (4).
These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).
(6) Subsection (e)(1).
It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) Subsection (e)(2).
To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigation.

(8) Subsection (e)(3).
To inform individuals as required by this subsection could reveal the existence of a criminal or civil investigation and compromise investigative efforts.

(9) Subsection (e)(5).
It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) Subsection (e)(8).
To serve notice could give persons sufficient warning to evade investigative efforts.

(11) Subsection (g).
This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(c) The following system of records is exempted from subsections (d)(1), (2), (3) and (4) of the Privacy Act pursuant to 5 U.S.C. 552a (k): “Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission (JUSTICE/CRT-007).” These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) Subsection (d)(1).
Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. In addition, these records may be subject to protective orders entered by federal courts to protect their confidentiality. Further, many of the records contained in this system are copies of documents which are the
property of state agencies and were obtained under express or implied promises to strictly protect their confidentiality.

(2) Subsection (d)(2).
Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(3) Subsection (d)(1), (2), (3) and (4).
This system contains investigatory material compiled by the Equal Opportunity Commission pursuant to its authority under 42 U.S.C. 2000e-8. Titles 42 U.S.C. 2000e-5(b), 42 U.S.C. 2000e-8(e), and 44 U.S.C. 3508 make it unlawful to make public in any manner whatsoever any information obtained by the Commission pursuant to the authority.

(4) Subsection (d)(3) and (4).
These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

Official Citation:

28 CFR Section 16.91: Exemption of Criminal Division Systems—limited access, as indicated.

(a) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a; in addition, the following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of 5 U.S.C. 552a:

(1) Central Criminal Division, Index File and Associated Records System of Records (JUSTICE/CRM-001)—Limited Access. This system of records and associated exemptions is adopted by and applies with equal force and effect to the National Security Division, until modified, superseded, or revoked in accordance with law.

(2) General Crimes Section, Criminal Division, Central Index File and Associated Records System of Records (JUSTICE/CRM-004)—Limited Access.

These exemptions apply to the extent that information in those systems are subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).
(b) The systems of records listed under paragraphs (b)(1) and (b)(2) of this section are exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3). (d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, or the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4). (e)(1). The notices of these systems of records published in the Federal Register set forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal or other law enforcement investigations, cases, and matters, the Criminal Division or its components will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.
(5). (e)(2). In a criminal investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6). (e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that these systems of records are exempted from subsections (f) and (d).

(8). (e)(4)(I). The categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9). (e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10). (e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.
(11). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to
the existence of records pertaining to him dealing with an actual or potential
criminal, civil, or regulatory investigation or prosecution must be exempted
because such notice to an individual would be detrimental to the successful
conduct and/or completion of an investigation or prosecution pending or future.
In addition, mere notice of the fact of an investigation could inform
the subject or others that their activities are under or may become the subject of an
investigation and could enable the subjects to avoid detection or apprehension, to
influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to
Records) the rules require pursuant to subsection (f) (2) through (5) are
inapplicable to these systems of records to the extent that these systems of
records are exempted from subsection (d).

(12). (g). Since an exemption is being claimed for subsections (d) (Access to
Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for
the reasons set forth for those subsections, to the extent that these systems of
records are exempted from subsections (d) and (f).

(13). In addition, exemption is claimed for these systems of records from
compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C.
552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): Subsections (c)(3), (d),
(e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in
these systems are specifically authorized to be kept secret in the interests of
national defense and foreign policy.

(c) The following system of records is exempted pursuant to the provisions of 5
U.S.C. 552a(j) (2) from subsection (c) (3) and (4), (d), (e)(1), (2) and (3), (e) (4)
(G), (H) and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a:

Source: Criminal Division Witness Security File System of
Records(JUSTICE/CRM-002).

These exemptions apply to the extent that information in this system is
subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(d) The system of records listed under paragraph (c) of this section is exempted,
for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3) The release of the disclosure accounting for disclosures made pursuant
to subsection (b) of the Act, including those permitted under the routine uses
published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, to determine whether he is the subject of a criminal investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, or the identity of witnesses and informants and the nature of their reports, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records. Moreover, disclosure of the disclosure accounting to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to obtain, and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

(2). (c)(4) Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d) Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, access to the records in these systems to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to obtain, and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

(4). Exemption is claimed from subsection (e)(1) for the reasons stated in subsection (b)(4) of this section.

(5). (e)(2) In the course of preparing a Witness Security Program for an individual, much of the information is collected from the subject. However, the requirement that the information be collected to the greatest extent practicable from the subject individual would present a serious impediment to criminal law enforcement because the individual himself may be the subject of a criminal investigation or have been a participant in, or observer of, criminal activity. As a result, it is necessary to seek information from other sources. In addition, the
failure to verify the information provided from the individual when necessary and to seek other information could jeopardize the confidentiality of the Witness Security Program and lead to the obtaining and maintenance of incorrect and uninvestigated information on criminal matters.

(6). (e)(3) The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise or reveal the identity of witnesses and informants protected under the Witness Security Program.

(7). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable.

(8). (e)(4)(I). The categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in the system, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal law, enforcement information and of witnesses and informants protected under the Witness Security Program.

(9). Exemption is claimed from subsections (e)(5) and (e)(8) for the reasons stated in subsection (b)(9) and (b)(10) of this section.

(10). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records contained in these systems pertaining to him would inform the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful conduct and/or completion of an investigation pending or future, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, notices as to the existence of records contained in these systems to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to obtain, and to
protect the confidentiality of, information compiled for purposes of a criminal investigation.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable.

(11). (g) Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable and is exempted for the reasons set forth for those subsections.

(e) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (4) (G), (H) and (I), (f), and (g) of 5 U.S.C. 552a:

Source: Organized Crime and Racketeering Section, Intelligence and Special Services Unit, Information Request System of Records (JUSTICE/CRM-014).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(f) The system of records listed under paragraph (e) of this section is exempted for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation to determine whether he is the subject of a criminal investigation and would therefore present a serious impediment to law enforcement. The records in these systems contain the names of the subjects of the files in question and the system is accessible by name of the person checking out the file and by name of the subject of the file. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation. This would present a serious impediment to effective law enforcement because it could prevent the successful completion of
the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4). Exemption is claimed from subsections (e)(4) (G), (H) and (I) for the reasons stated in subsections (b)(7) and (b)(8) of this section.

(5). (f). These systems may be accessed by the name of the person who is the subject of the file and who may also be the subject of a criminal investigation. Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him, which may deal with an actual or potential criminal investigation or prosecution, must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of the investigation or prosecution pending or future. In addition mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable.

(6). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) of the Act this section is inapplicable and is exempted for the reasons set forth for those subsections.

(g) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(4), (d), (e)(4) (G), (H) and (I), (f) and (g) of 5 U.S.C. 552a.

Source: File of Names Checked to Determine If Those Individuals Have Been the Subject of an Electronic Surveillance System of Records (JUSTICE/CRM-003).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(h) The system of records listed under paragraph (g) of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:
(1). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable to the extent that this system of records is exempted from subsection (d).

(2). (d). The records contained in this system of records generally consist of information filed with the court in response to the request and made available to the requestor. To the extent that these records have been so filed, no exemption is sought from the provisions of this subsection. Occasionally, the records contain pertinent logs of intercepted communications and other investigative reports not filed with the court. These records must be exempted because access to such records could inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation and of the nature of the information and evidence obtained by the government. This would present a serious impediment to effective law enforcement because it could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(3). Exemption is claimed from subsections (e)(4) (G), (H) and (I) for the reasons stated in subsections (b)(7) and (b)(8) of this section.

(4). (f). The records contained in this system of records generally consist of information filed with the court and made available to the requestor. To the extent that these records have been so filed, no exemption is sought from the provisions of this subsection. Occasionally, the records contain pertinent logs of intercepted communications and other investigative reports not filed with the court. These records must be exempted from a requirement of notification as to their existence because such notice to an individual would be detrimental to the successful conduct and/or completion of a criminal investigation or prosecution pending or future. In addition, mere notice of the existence of such logs or investigative reports could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable to the extent that this system of records is exempted for subsection (d).

(6). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that this system of records is exempted from subsections (d) and (f).
(i) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2), and (3), (e)(4) (G), (H), and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a:

(1) Information File on Individuals and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities System of Records (JUSTICE/CRM-006).

(2) The Stocks and Bonds Intelligence Control Card File System of Records (JUSTICE/CRM-021).

(3) Tax Disclosure Index File and Associated Records (JUSTICE/CRM-025).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(j) The systems of records listed in paragraphs (i)(1), (i)(2), and (i)(3) of this section are exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3) The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation to determine whether he is the subject of a criminal investigation, to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for this system of records.

(2)(c)(4) Since an exemption is being claimed for subsection (d) of the act (access to records), this section is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3)(d) Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead
to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4) Exemption is claimed from subsections (e)(1), (2), and (3), (e)(4) (G), (H), and (I), (e)(5) and (e)(8) for the reasons stated in subsections (b)(4), (b)(5), (b)(6), (b)(7), (b)(8), (b)(9), and (b)(10) of this section.

(5)(f) Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Since an exemption is being claimed for subsection (d) of the act (access to records), the rules required pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records.

(6)(g) Since an exemption is being claimed for subsections (d) (access to records) and (f) (Agency rules), this section is inapplicable and is exempted for the reasons set forth for those subsections.

(k) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a; in addition, the following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) from subsections (c) (3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) of 5 U.S.C. 552a:

Source: Organized Crime and Racketeering Section, Criminal Division, General Index File and Associated Records System of Records (JUSTICE/CRM-012).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(1).
(l) The system of records listed under paragraph (m)\(^2\) of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). Exemption is claimed from subsections (c) (3) and (4) and (d) for the reasons stated in subsections (j)(1), (j)(2) and (j)(3) of this section.

(2). (e)(1). The notice for this system of records published in the Federal Register sets forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal investigations, cases, and matters, the Organized Crime and Racketeering Section will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority, or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in this system of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(3). Exemption is claimed from subsections (e) (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f) and (g) for the reasons stated in subsections (b)(5), (b)(6), (b)(7), (b)(8), (b)(9), (b)(10), (b)(11) and (b)(12) of this section.

(4). In addition, exemption is claimed for this system of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): Subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in this system are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(m) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (2) and (3), (e) (4) (G), (H) and (I), (e) (8), (f) and (g) of 5 U.S.C. 552a:

---

\(^2\) Paragraph (m) was redesignated as paragraph (k) at 44 FR 54046, Sept. 18, 1979.
These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(n) The system of records listed in paragraph (m) of this section is exempted for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

1. (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an electronic interception to obtain valuable information concerning the interception, including information as to whether he is the subject of a criminal investigation, by means other than those provided for by statute. Such information could interfere with the successful conduct and/or completion of a criminal investigation, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

2. (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

3. (d). Access to the records contained in these systems would inform the subject of an electronic interception of the existence of such surveillance including information as to whether he is the subject of a criminal investigation by means other than those provided for by statute. This could interfere with the successful conduct and/or completion of a criminal investigation and therefore present a serious impediment to law enforcement.

4. (e)(2). In the context of an electronic interception, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and this would therefore destroy the efficacy of the interception.

5. (e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence
of a confidential electronic interception or reveal the identity of witnesses or confidential informants.

(6). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable.

(7). Exemption is claimed from subsections (e)(4)(I) and (e)(8) for the reasons stated in subsections (b)(8) and (b)(10) of this section.

(8). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an electronic interception other than pursuant to statute must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation pending or future. In addition, mere notice of the fact of an electronic interception could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f)(2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(9). (g). Since an exemption is being claimed for subsection (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsection (d) and (f).

(o) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (2) and (3), (e) (4) (G), (H), and (I), (e)(8), (f) and (g) of 5 U.S.C. 552a; in addition the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), (e)(4) (G), (H) and (I), and (f) of 5 U.S.C. 552a:


These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(1) and (k)(2).
(p) The system of records listed under paragraph (q)\(^3\) of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). Release of the accounting of disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for this system of records, (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus creating a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activities, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable to the extent that this system of records is exempted from subsection (d).

(3). (d). Access to the records contained in this system (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus presenting a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activities, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

(4). (e)(2). In a witness immunity request matter, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the immunity request and often the subject of the underlying investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

---

\(^3\) Paragraph (q) was redesignated as paragraph (o) at 44 FR 54046, Sept. 18, 1979.
(5). Exemption is claimed from subsections (e)(3), (e)(4)(G), (H) and (I), and (e)(8) for the reasons stated in subsections (b)(6), (b)(7), (b)(8) and (b)(10) of this section.

(6). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus presenting a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activity, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f)(2) through (5) are inapplicable to this system of records to the extent that this system of records is exempted from subsection (d).

(7). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that this system of records is exempted for subsections (d) and (f).

(8). In addition, exemption is claimed for this system of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in this system are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(q) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f), and (g):

(1) Freedom of Information/Privacy Act Records (JUSTICE/CRM-024)

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(r) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, it is exempted for the reasons set forth from the following provisions of 5 U.S.C. 552a:
(1)(c)(3). The release of the disclosure accounting would present a serious impediment to law enforcement by permitting the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation and the information obtained, or to identify witnesses and informants.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records), this subsection is inapplicable to the extent that this system of records is exempted from subsection (d).

(3)(d). Access to records contained in this system would enable the subject of an investigation of an actual or potential criminal or civil case or regulatory violation to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature and scope of the investigation, and information or evidence obtained as to his/her activities, to identify witnesses and informants, or to avoid detection or apprehension. Such results could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony, and thereby present a serious impediment to effective law enforcement. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4)(e)(1). In the course of criminal or other law enforcement investigations, cases, and matters, the Criminal Division will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority, or it may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(5)(e)(2). To collect information to the greatest extent practicable from the subject individual of a criminal investigation or prosecution would present a serious impediment to law enforcement. The nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) (e)(3). To provide individuals supplying information with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a
confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). These subsections are inapplicable to the extent that this system is exempt from the access provisions of subsection (d) and the rules provisions of subsection (f).

(8)(e)(4)(I). The categories of sources of the records in this system have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in this system, exemption from this provision is necessary to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9) (e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would inhibit the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). This subsection is inapplicable to the extent that this system is exempt from the access provisions of subsection (d).

(12)(g). Because some of the records in this system contain information which was compiled for law enforcement purposes and have been exempted from the access provisions of subsection (d), subsection (g) is inapplicable.

(s) The following system of records is exempted from 5 U.S.C. 552a(d).

Source: Office of Special Investigations Displaced Persons Listings (JUSTICE/CRM-027).
This exemption applies to the extent that the records in this system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(t) Exemption from subsection (d) is justified for the following reasons:

(1) Access to records contained in this system could inform the subject of the identity of witnesses or informants. The release of such information could present a serious impediment to effective law enforcement by endangering the physical safety of witnesses or informants; by leading to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony; or by otherwise preventing the successful completion of an investigation.

(u) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j) and/or (k) from subsections (c)(3) and (4); (d)(1), (d)(2), (d)(3) and (d)(4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (e)(5) and (e)(8); (f), and (g) of 5 U.S.C. 552a: Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System (JUSTICE/CRM-028). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k).

(v) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation by the Organized Crime Drug Enforcement Task Force Fusion Center, the International Organized Crime Intelligence and Operations Center, or the recipient agency, and could permit that individual to take measures to avoid detection or apprehension, to learn the identity of witnesses and informants, or to destroy evidence, and would therefore present a serious impediment to law enforcement or counterintelligence efforts. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record. Moreover, release of an accounting may reveal information that is properly classified pursuant to Executive Order and could compromise the national defense or foreign policy.

(2) From subsection (c)(4) because this subsection is inapplicable to the extent that an exemption is being claimed from subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of records in the system could alert the subject of an actual or potential criminal, civil, or regulatory
investigation of the existence of that investigation, of the nature and scope of the
information and evidence obtained as to his activities, of the identity of
confidential witnesses and informants, of the investigative interest of the
Organized Crime Drug Enforcement Task Force Fusion Center, International
Organized Crime Intelligence and Operations Center, and other intelligence or
law enforcement agencies (including those responsible for civil proceedings
related to laws against drug trafficking or related financial crimes or international
organized crime); lead to the destruction of evidence, improper influencing of
witnesses, fabrication of testimony, and/or flight of the subject; reveal the details
of a sensitive investigative or intelligence technique, or the identity of a
confidential source; or otherwise impede, compromise, or interfere with
investigative efforts and other related law enforcement and/or intelligence
activities. In addition, disclosure could invade the privacy of third parties and/or
endanger the life, health, and physical safety of law enforcement personnel,
confidential informants, witnesses, and potential crime victims. Access to records
could also result in the release of information properly classified pursuant to
Executive Order, thereby compromising the national defense or foreign policy.

(4) From subsection (d)(2) because amendment of the records thought to be incorrect, irrelevant, or untimely would also interfere with ongoing
investigations, criminal or civil law enforcement proceedings, and other law
enforcement activities and impose an impossible administrative burden by
requiring investigations, analyses, and reports to be continuously reinvestigated
and revised, as well as impact information properly classified pursuant to
Executive Order.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because, in the course of its acquisition,
collation, and analysis of information under the statutory authority granted to
them, both the Organized Crime Drug Enforcement Task Force Fusion Center
and International Organized Crime Intelligence and Operations Center will
occasionally obtain information, including information properly classified
pursuant to Executive Order, that concern actual or potential violations of law
that are not strictly within its statutory or other authority or may compile
information in the course of an investigation which may not be relevant to a
specific prosecution. It is impossible to determine in advance what information
collected during an investigation will be important or crucial to the apprehension
of fugitives. In the interests of effective law enforcement, it is necessary to retain
such information in this system of records because it can aid in establishing
patterns of criminal activity and can provide valuable leads for federal and other
law enforcement agencies. This consideration applies equally to information
acquired from, or collated or analyzed for, both law enforcement agencies and
agencies of the U.S. foreign intelligence community and military community.
(7) From subsection (e)(2) because in a criminal, civil, or regulatory investigation, prosecution, or proceeding, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation, prosecution, or proceeding would be placed on notice as to the existence and nature of the investigation, prosecution, and proceeding and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Moreover, thorough and effective investigation and prosecution may require seeking information from a number of different sources.

(8) From subsection (e)(3) (to the extent applicable) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants and endanger their lives, health, and physical safety. The individual could seriously interfere with undercover investigative techniques and could take appropriate steps to evade the investigation or flee a specific area.

(9) From subsections (e)(4)(G), (H) and (I) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(10) From subsection (e)(5) because the acquisition, collation, and analysis of information for law enforcement purposes from various agencies does not permit a determination in advance or a prediction of what information will be matched with other information and thus whether it is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys to exercise their judgment in collating and analyzing information and would impede the development of criminal or other intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement by revealing investigative techniques, procedures, evidence, or interest and interfering with the ability to issue warrants or subpoenas, and could give persons sufficient warning to evade investigative efforts.

Page 370
(12) From subsections (f) and (g) because these subsections are inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:

28 CFR Section 16.92: Exemption of Environment and Natural Resources Division Systems—limited access.

(a)(1) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(5), (e)(8), (f) and (g); in addition, the following systems of records are exempted pursuant to 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1):

(i) Environment and Natural Resources Division Case and Related Files System, JUSTICE/ENRD-003.

(ii) [Reserved]

(2) These exemptions apply only to the extent that information in this system relates to the investigation, prosecution or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy, and therefore is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigations, and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law or regulatory enforcement process, the applicable exemption may be waived by the Environment and Natural Resources Division.

(b) Only that information that relates to the investigation, prosecution or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy is exempted for the reasons set forth from the following subsections:

(i) Subsection (e)(3).
Subsection (c)(3) requires an agency to provide an accounting of disclosures of records concerning an individual. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records would inform that individual (and others to whom the subject might disclose the records) of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and others to avoid criminal penalties and civil remedies.

(2) Subsections (c)(4) (requiring an agency to inform individuals about any corrections made to a record that has been disclosed) and (g) (providing for civil remedies when an agency fails to comply with these provisions).

These provisions are inapplicable to the extent that this system of records is exempted from subsection (d).

(3) Subsection (d).

Subsection (d) requires an agency to allow individuals to gain access to a record about him or herself; to dispute the accuracy, relevance, timeliness or completeness of such records; and to have an opportunity to amend his or her record or seek judicial review. To the extent that information contained in this system has been properly classified, relates to the investigation and/or prosecution of grand jury, civil fraud, and other law enforcement matters, disclosure could compromise matters which should be kept secret in the interest of national security or foreign policy; compromise confidential investigations or proceedings; impede affirmative enforcement actions based upon alleged violations of regulations or of civil or criminal laws; reveal the identity of confidential sources; and result in unwarranted invasions of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) Subsection (e)(1).

Subsection (e)(1) requires an agency to maintain in its records only such information about an individual that is relevant and necessary to accomplish the agency's purpose. In the course of criminal or civil investigations, cases, or other matters, the Environment and Natural Resources Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.
(5) Subsection (e)(2).

Subsection (e)(2) requires an agency to collect information to the greatest extent practicable from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs. To collect information from the subject of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject (and others with whom the subject might be in contact) would be informed of the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) Subsection (e)(3).

Subsection (e)(3) requires an agency to inform each individual whom it asks to supply information, on a form that can be retained by the individual, the authority which authorizes the solicitation, the principal purpose for the information, the routine uses of the information, and the effects on the individual of not providing the requested information. To comply with this requirement during the course of a criminal investigation or prosecution could jeopardize the investigation by disclosing the existence of a confidential investigation, revealing the identity of witnesses or confidential informants, or impeding the information gathering process.

(7) Subsection (e)(5).

Subsection (e)(5) requires an agency to maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual. In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(8) Subsection (e)(8).

Subsection (e)(8) requires agencies to make reasonable efforts to serve notice on an individual when any record on the individual is made available to any person under compulsory legal process. To serve notice would give persons sufficient warning to evade law enforcement efforts.
(9) Subsections (f) and (g).

Subsection (f) requires an agency to establish procedures to allow an individual to have access to information about him or herself and to contest information kept by an agency about him or herself. Subsection (g) provides for civil remedies against agencies who fail to comply with the Privacy Act requirements. These provisions are inapplicable to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(c) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (d):

(1) Freedom of Information/Privacy Act Records System. (Justice/LDN-005).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c) (3) because that portion of the Freedom of Information/Privacy Act Records System that consists of investigatory materials compiled for law enforcement purposes is being exempted from access and contest; the provision for disclosure of accounting is not applicable.

(2) From subsection (d) because of the need to safeguard the identity of confidential informants and avoid interference with ongoing investigations or law enforcement activities by preventing premature disclosure of information relating to those efforts.

Official Citation:

28 CFR Section 16.93: Exemption of Tax Division Systems—limited access.

(a) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3), (e)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f) and (g) of 5 U.S.C. 552a:
(1) Tax Division Central Classification Cards, Index Docket Cards, and Associated Records—Criminal Tax Cases (JUSTICE/TAX-001)—Limited Access.

(2) These exemptions apply to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) The system of records listed under paragraph (a)(1) of this section is exempted for the reasons set forth below, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting, for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for those systems of records, would enable the subject of an investigation of an actual or potential criminal tax case to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, and to determine the identity of witnesses or informants. Such access to investigative information would, accordingly, present a serious impediment to law enforcement. In addition, disclosure of the accounting would constitute notice to the individual of the existence of a record even though such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3) (d)(1); (d)(2); (d)(3); (d)(4). Access to the records contained in these systems would inform the subject of an actual or potential criminal tax investigation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his or her activities, and of the identity of witnesses or informants. Such access would, accordingly, provide information that could enable the subject to avoid detection, apprehension and prosecution. This result, therefore, would constitute a serious impediment to effective law enforcement not only because it would prevent the successful completion of the investigation but also because it could endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4)(e)(1). The notices for these systems of records published in the Federal Register, set forth the basic statutory or related authority for maintenance of these systems. However, in the course of criminal tax and related law enforcement investigations, cases, and matters, the Tax Division will occasionally obtain information concerning actual or potential violations of law that may not be technically within its statutory or other authority or may compile information
in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain some or all of such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(5)(e)(2). In a criminal tax investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, influence witnesses improperly, destroy evidence, or fabricate testimony.

(6)(e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that these systems of records are exempted from subsection (f) and (d).

(8)(e)(4)(I). The categories of sources of the records in the systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal tax and related law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9)(e)(5). In the collection of information for criminal tax enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. Furthermore, the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal tax information and related data necessary for effective law enforcement.
(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal tax, civil tax, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion or an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(12)(g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(c) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G, (e)(4)(H, (e)(4)(I) and (f) of 5 U.S.C. 552a:

(1) Tax Division Central Classification Cards, Index Docket Cards, and Associated Records—Civil Tax Cases (JUSTICE/TAX-002)—Limited Access.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(d) The system of records listed under paragraph (c)(1) is exempted for the reasons set forth below, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting, for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for this system of records, would enable the subject of an investigation of an actual or potential civil tax case to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, and to determine the identity of
witnesses or informants. Such access to investigative information would, accordingly, present a serious impediment to law enforcement. In addition, disclosure of the accounting would constitute notice to the individual of the existence of a record even though such notice requirement under subsection (f)(1) is specifically exempted for this system of records.

(2)(d)(1); (d)(2); (d)(3); (d)(4). Access to the records contained in this system would inform the subject of an actual or potential civil tax investigation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his or her activities and of the identity of witnesses or informants. Such access would, accordingly, provide information that could enable the subject to avoid detection. This result, therefore, would constitute a serious impediment to effective law enforcement not only because it would prevent the successful completion of the investigation but also because it could endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(3)(e)(1). The notices for this system of records published in the Federal Register set forth the basic statutory or related authority for maintenance of this system. However, in the course of civil tax and related law enforcement investigations, cases and matters, the Tax Division will occasionally obtain information concerning actual or potential violations of law that are not strictly or technically within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific case. In the interests of effective law enforcement, it is necessary to retain some or all of such information in this system of records since it can aid in establishing patterns of tax compliance and can provide valuable leads for Federal and other law enforcement agencies.

(4)(e)(4)(G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that this system of records is exempted from subsection (f) and (d).

(5)(e)(4)(I). The categories of sources of the records in this system have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in this system, exemption from this provision is necessary in order to protect the confidentiality of the sources of civil tax and related law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.
(6)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to existence of records pertaining to the individual dealing with an actual or potential criminal tax, civil tax, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or case, pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable to this system of records to the extent that this system of records is exempted from subsection (d).

(e) The following system of records is exempt from subsections (c)(3) and (d)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5): Files of Applicants for Attorney and Non-Attorney Positions with the Tax Division, Justice/TAX-003. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(f) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because an accounting could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a position with the Tax Division. Disclosure of an accounting could reveal the identity of a source of information and constitutes a breach of the promise of confidentiality by the Tax Division. This would result in the reduction in the free flow of information vital to a determination of an applicant's qualifications and suitability for federal employment.

(2) From subsection (d)(1) because disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a Tax Division position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Tax Division. Such breaches ultimately would restrict the free flow of information vital to a determination of an applicant's qualifications and suitability.

Official Citation:

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g):

(1) Central Records System (CRS) (JUSTICE/FBI-002).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552(j) and (k). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by the FBI.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.

(2)(i) From subsections (d), (e)(4) (G) and (H), (f) and (g) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information classified in the interest of national security, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety to law enforcement personnel.

(ii) Also, individual access to non-criminal investigative records, e.g., civil investigations and administrative inquiries, as described in subsection (k) of the Privacy Act, could also compromise classified information related to national security, interfere with a pending investigation or internal inquiry, constitute an unwarranted invasion of privacy, reveal a confidential source or sensitive investigative technique, or pose a potential threat to law enforcement personnel. In addition, disclosure of information collected pursuant to an
employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the objectivity or fairness of a testing or examination process.

(iii) In addition, from paragraph (d)(2) of this section, because to require the FBI to amend information thought to be incorrect, irrelevant or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(3) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) In any investigation the FBI might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

(4) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(5) From subsection (e)(3) because disclosure would provide the subject with substantial information which could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take appropriate steps to evade the investigation or flee a specific area.
(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

(7) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(c) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (m):


These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of accounting disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, resulting in a serious impediment to law enforcement.

(2) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) because these provisions concern an individual's access to records which concern him and such access to records in this system would compromise ongoing investigations, reveal investigatory techniques and confidential informants, and invade the privacy of private citizens who provide information in connection with a particular investigation.

(3) From subsection (e)(1) because these indices must be maintained in order to provide the information as described in the “routine uses” of this particular system.

(4) From subsections (e) (2) and (3) because compliance is not feasible given the subject matter of the indices.
(5) From subsection (e)(5) because this provision is not applicable to the indices in view of the “routine uses” of the indices. For example, it is impossible to predict when it will be necessary to utilize information in the system and, accordingly it is not possible to determine when the records are timely.

(6) From subsection (e)(8) because the notice requirement could present a serious impediment to law enforcement by revealing investigative techniques, procedures and the existence of confidential investigations.

(7) From subsection (m) for the reasons stated in subsection (b)(7) of this section.

(e) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Identification Division Records System (JUSTICE/FBI-009).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j).

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) for the reasons stated in subsection (d)(1) of this section.

(2) From subsections (c)(4), (d), (e)(4) (G) and (H), (f) and (g) because these provisions concern an individual's access to records which concern him. Such access is directed at allowing the subject of a record to correct inaccuracies in it. Although an alternate system of access has been provided in 28 CFR 16.30 to 34 and 28 CFR 20.34, the vast majority of records in this system concern local arrests which it would be inappropriate for the FBI to undertake to correct.

(3) From subsection (e)(1) because it is impossible to state with any degree of certainty that all information on these records is relevant to accomplish a purpose of the FBI, even though acquisition of the records from state and local law enforcement agencies is based on a statutory requirement. In view of the number of records in the system it is impossible to review them for relevancy.

(4) From subsection (e)(2) because the records in the system are necessarily furnished by criminal justice agencies due to their very nature.
(5) From subsection (e)(3) because compliance is not feasible due to the nature of the records.

(6) From subsection (e)(5) because the vast majority of these records come from local criminal justice agencies and it is administratively impossible to ensure that the records comply with this provision. Submitting agencies are, however, urged on a continuing basis to ensure that their records are accurate and include all dispositions.

(7) From subsection (e)(8) because the FBI has no logical manner to ascertain whether process has been made public and compliance with this provision would in any case, provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures or evidence.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) and (H), (e)(5), (e)(8), (f), and (g):

1) National Crime Information Center (NCIC) (JUSTICE/FBI-001). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(3).

(h) Exemptions from the particular subsections are justified for the following reasons:

1) From subsection (c)(3) for the reasons stated in subsection (d)(1) of this section.

2) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) for the reasons stated in subsection (d)(2) of this section. When records are properly subject to access by the individual, an alternate means of access is provided in subsection (i) of this section.

3) From subsection (e)(1) because information contained in this system is primarily from state and local records, and it is for the official use of agencies outside the Federal Government in accordance with 28 U.S.C. 534.

4) From subsections (e) (2) and (3) because it is not feasible to comply with these provisions given the nature of this system.

5) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to
exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, the vast majority of these records come from other federal, state, local, joint, foreign, tribal, and international agencies and it is administratively impossible to ensure that the records comply with this provision. Submitting agencies are, however, urged on a continuing basis to ensure that their records are accurate and include all dispositions.

(6) From subsection (e)(8) for the reasons stated in subsection (d)(6) of this section.

(i) Access to computerized criminal history records in the National Crime Information Center is available to the individual who is the subject of the record pursuant to procedures and requirements specified in the Notice of Systems of Records compiled by the National Archives and Records Service and published under the designation:

(j) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G) and (H), (e)(5), (f) and (g):

(1) National Center for the Analysis of Violent Crime (NCAVC) (JUSTICE/FBI-015).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(k) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because providing the accounting of disclosures to the subject could prematurely reveal investigative interest by the FBI and other law enforcement agencies, thereby providing the individual an opportunity to impede an active investigation, destroy or alter evidence, and possibly render harm to violent crime victims and/or witnesses.

(2) From subsections (d), (e)(4) (G) and (H), and (f) because disclosure to the subject could interfere with enforcement proceedings of a criminal justice agency, reveal the identity of a confidential source, result in an unwarranted invasion of another's privacy, reveal the details of a sensitive investigative technique, or endanger the life and safety of law enforcement personnel, potential violent crime victims, and witnesses. Disclosure also could prevent the future apprehension of a violent or exceptionally dangerous criminal fugitive should he or she modify his or her method of operation in order to evade law enforcement. Also, specifically from subsection (d)(2), which permits an
individual to request amendment of a record, because the nature of the information in the system is such that an individual criminal offender would frequently demand amendment of derogatory information, forcing the FBI to continuously retrograde its criminal investigations in an attempt to resolve questions of accuracy, etc.

(3) From subsection (g) because the system is exempt from the access and amendment provisions of subsection (d).

(4) From subsection (e)(1) because it is not always possible to establish relevance and necessity of the information at the time it is obtained or developed. Information, the relevance and necessity of which may not be readily apparent, frequently can prove to be of investigative value at a later date and time.

(5) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

(l) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d), (e)(1), (2), and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g).

(1) FBI Counterdrug Information Indices System (CIIS) (JUSTICE/FBI—016)

(2) [Reserved]

(m) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.
(2) From subsection (c)(4) to the extent it is not applicable because an exemption is being claimed from subsection (d).

(3)(i) From subsections (d), (e)(4) (G) and (H) because these provisions concern individual access to records, compliance with which could compromise sensitive information, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

   (ii) In addition, from paragraph (d), because to require the FBI to amend information thought to be incorrect, irrelevant or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4)(i) From subsection (e)(1) because it is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

   (ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed otherwise. It is only after the information is assessed that its relevancy and necessity in a specified investigative activity can be established.

   (iii) In any investigation the FBI might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

   (iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual often can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to principally rely upon information furnished by the individual concerning his own activities.
(6) From subsection (e)(3) because disclosure would provide the subject with information which could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take appropriate steps to evade the investigation or flee a specific area.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(9) From subsection (f) to the extent that this system is exempt from the provisions of subsection (d).

(10) From subsection (g) to the extent that this system of records is exempt from the provisions of subsection (d).

(n) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4); (d); (e)(1), (2), and 3; (e)(4) (G) and (H); (e) (5) and (8); and (g):

(1) National DNA Index System (NDIS) (JUSTICE/FBI-017).

(2) [Reserved]

(o) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available the accounting of disclosures of records to the subject of the record would prematurely place the subject on notice of the investigative interest of law enforcement agencies, provide the subject with significant information concerning the nature of the investigation, or permit the subject to take measures to impede the investigation (e.g., destroy or alter evidence, intimidate potential witnesses, or flee the area to avoid investigation and prosecution), and result in a serious impediment to law enforcement.
(2)(i) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) because these provisions concern an individual’s access to records which concern him/her and access to records in this system would compromise ongoing investigations. Such access is directed at allowing the subject of the record to correct inaccuracies in it. The vast majority of records in this system are from the DNA records of local and State NDIS agencies which would be inappropriate and not feasible for the FBI to undertake to correct. Nevertheless, an alternate method to access and/or amend records in this system is available to an individual who is the subject of a record pursuant to procedures and requirements specified in the Notice of Systems of Records compiled by the National Archives and Records Administration and published in the Federal Register under the designation: National DNA Index System (NDIS) (JUSTICE/FBI-017)

(ii) In addition, from paragraph (d)(2) of this section, because to require the FBI to amend information thought to be incorrect, irrelevant, or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde investigations attempting to resolve questions of accuracy, etc.

(iii) In addition, from subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

(3) From subsection (e)(1) because:

(i) Information in this system is primarily from State and local records and it is for the official use of agencies outside the Federal Government.

(ii) It is not possible in all instances to determine the relevancy or necessity of specific information in the early stages of the criminal investigative process.

(iii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary, and vice versa. It is only after the information is assessed that its relevancy in a specific investigative activity can be established.

(iv) Although the investigative process could leave in doubt the relevancy and necessity of evidence which had been properly obtained, the same information could be relevant to another investigation or investigative activity under the jurisdiction of the FBI or another law enforcement agency.

(4) From subsections (e)(2) and (3) because it is not feasible to comply with these provisions given the nature of this system. Most of the records in this system are necessarily furnished by State and local criminal justice agencies and not by individuals due to the very nature of the records and the system.
(5) From subsection (e)(5) because the vast majority of these records come from State and local criminal justice agencies and because it is administratively impossible for them and the FBI to insure that the records comply with this provision. Submitting agencies are urged and make every effort to insure records are accurate and complete; however, since it is not possible to predict when information in the indexes of the system (whether submitted by State and local criminal justice agencies or generated by the FBI) will be matched with other information, it is not possible to determine when most of them are relevant or timely.

(6) From subsection (e)(8) because the FBI has no logical manner to determine whenever process has been made public and compliance with this provision would provide an impediment to law enforcement by interfering with ongoing investigations.

(p) The National Instant Criminal Background Check System (NICS), (JUSTICE/FBI-018), a Privacy Act system of records, is exempt:

(1) Pursuant to 5 U.S.C. 552a(j)(2), from subsections (c)(3) and (4); (d); (e)(1), (2) and (3); (e)(4) (G) and (H); (e)(5) and (8); and (g); and

(2) Pursuant to 5 U.S.C. 552a(k)(2) and (3), from subsections (c)(3), (d), (e)(1), and (e)(4) (G) and (H).

(q) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2), and (k)(3). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the accounting of disclosures would place the subject on notice that the subject is or has been the subject of investigation and result in a serious impediment to law enforcement.

(2) From subsection (c)(4) to the extent that it is not applicable since an exemption is claimed from subsection (d).

(3) From subsections (d) and (e)(4) (G) and (H) because these provisions concern an individual’s access to records which concern the individual and such access to records in the system would compromise ongoing investigations, reveal investigatory techniques and confidential informants, invade the privacy of persons who provide information in connection with a particular investigation, or constitute a potential danger to the health or safety of law enforcement personnel.
(ii) In addition, from subsection (d)(2) because, to require the FBI to amend information thought to be not accurate, timely, relevant, and complete, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative burden by forcing the agency to continuously update its investigations attempting to resolve these issues.

(iii) Although the Attorney General is exempting this system from subsections (d) and (e)(4)(G) and (H), an alternate method of access and correction has been provided in 28 CFR, part 25, subpart A.

(4) From subsection (e)(1) because it is impossible to state with any degree of certainty that all information in these records is relevant to accomplish a purpose of the FBI, even though acquisition of the records from state and local law enforcement agencies is based on a statutory requirement. In view of the number of records in the system, it is impossible to review them for relevancy.

(5) From subsections (e)(2) and (3) because the purpose of the system is to verify information about an individual. It would not be realistic to rely on information provided by the individual. In addition, much of the information contained in or checked by this system is from Federal, State, and local criminal history records.

(6) From subsection (e)(5) because it is impossible to predict when it will be necessary to use the information in the system, and, accordingly, it is not possible to determine in advance when the records will be timely. Since most of the records are from State and local or other Federal agency records, it would be impossible to review all of them to verify that they are accurate. In addition, an alternate procedure is being established in 28 CFR, part 25, subpart A, so the records can be amended if found to be incorrect.

(7) From subsection (e)(8) because the notice requirement could present a serious impediment to law enforcement by revealing investigative techniques and confidential investigations.

(8) From subsection (g) to the extent that, pursuant to subsections (j)(2), (k)(2), and (k)(3), the system is exempted from the other subsections listed in paragraph (p) of this section.

(r) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g):

(1) Terrorist Screening Records System (TSRS) (JUSTICE/FBI-

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2).
Where compliance would not appear to interfere with or adversely affect the counterterrorism purposes of this system, and the overall law enforcement process, the applicable exemption may be waived by the FBI in its sole discretion.

(s) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he/she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation. Similarly, disclosing this information to individuals who have been misidentified as known or suspected terrorists due to a close name similarity could reveal the Government’s investigative interest in a terrorist suspect, because it could make known the name of the individual who actually is the subject of the Government’s interest. Consequently, the Government has as great an interest in protecting the confidentiality of identifying information of misidentified persons as it does in protecting the confidentiality of the identities of known or suspected terrorists.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of records contained in this system, which consists of counterterrorism, investigatory and intelligence records. Compliance with these provisions could alert the subject of a terrorism investigation of the fact and nature of the investigation, and/or the investigative interest of the FBI and/or other intelligence or law enforcement agencies; compromise sensitive information classified in the interest of national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. Similarly, compliance with these provisions with respect to records on individuals who have been misidentified as known or suspected terrorists due to a close name similarity
could reveal the Government's investigative interest in a terrorist suspect, because it could make known the name of the individual who actually is the subject of the Government's interest.

(4) From subsection (e)(1) because it is not always possible for TSC to know in advance what information is relevant and necessary for it to complete an identity comparison between the individual being screened and a known or suspected terrorist. Also, because TSC and the FBI may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3), to the extent that this subsection is interpreted to require TSC to provide notice to an individual if TSC receives information about that individual from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsection (e)(5) because many of the records in this system are derived from other domestic and foreign agency record systems and therefore it is not possible for the FBI and the TSC to vouch for their compliance with this provision; however, the TSC has implemented internal quality assurance procedures to ensure that TSC terrorist screening data is as thorough, accurate, and current as possible. In addition, TSC supports but does not conduct investigations; therefore, it must be able to collect information related to terrorist identities and encounters for distribution to law enforcement and intelligence agencies that do conduct terrorism investigations. In the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their
judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. The TSC has, however, implemented internal quality assurance procedures to ensure that TSC terrorist screening data is as thorough, accurate, and current as possible. The FBI also is exempting the TSRS from the requirements of subsection (e)(5) in order to prevent the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the TSRS. The FBI has exempted TSRS records from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of counterterrorism investigations. Exempting the TSRS from subsection (e)(5) serves to prevent the assertion of challenges to a record's accuracy, timeliness, completeness, and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the FBI and the TSC and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(t) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act:

(1) Law Enforcement National Data Exchange (N-DEx), (JUSTICE/FBI-020).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the FBI in its sole discretion.

(u) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative interest in the individual. Revealing this information may thus compromise ongoing law enforcement efforts. Revealing this information may also permit the record subject to take measures to impede the investigation, such as destroying evidence, intimidating potential witnesses or fleeing the area to avoid the investigation.
(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4), because these provisions concern individual access to and amendment of investigatory records, compliance with which could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of the FBI and other law enforcement agencies; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing investigations and other law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes and, in fact, a major tenet of the N-DEx information sharing system is that the relevance of certain information may not always be evident in the absence of the ability to correlate that information with other existing law enforcement data.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to efforts to solve crimes and improve homeland security in that it would put the subject of an investigation on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(6) From subsection (e)(3) because disclosure would put the subject of an investigation on notice of that fact and would permit the subject to engage in conduct intended to thwart that activity.

(7)(i) From subsection (e)(5) because many of the records in this system are records contributed by other agencies and the restrictions imposed by (e)(5) would limit the utility of the N-DEx system. All data contributors are expected to ensure that information they share is relevant, timely, complete and accurate. In fact, rules for use of the N-DEx system will require that information be updated periodically and not be used as a basis for action or disseminated beyond the recipient without the recipient first obtaining permission from the record owner/contributor. These rules will be enforced through robust audit procedures.
The existence of these rules should ameliorate any perceived concerns about the integrity of the information in the N-DEx system. Nevertheless, exemption from this provision is warranted in order to reduce the administrative burden on the FBI to vouch for compliance with the provision by all N-DEx data contributors and to encourage those contributors to share information the significance of which may only become apparent when combined with other information in the N-DEx system.

(ii) The FBI is also exempting the N-DEx from subsection (e)(5) in order to block the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the N-DEx. The FBI has exempted these records from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of law enforcement investigations. Exempting the N-DEx system from subsection (e)(5) complements this exemption and will provide the FBI with the ability to prevent the assertion of challenges to a record’s accuracy, timeliness, completeness and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8), because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the FBI and may alert the subjects of law enforcement investigations to the fact of those investigations, when not previously known.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(v) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2) and (3); (e)(4)(G), (H) and (I); (e)(5) and (8); (f) and (g) of the Privacy Act:

(1) Data Integration and Visualization System (DIVS), (JUSTICE/FBI-021).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k). Where compliance would not appear to interfere with or adversely affect the intelligence and law enforcement purpose of this system, and the overall law enforcement process, the applicable exemption may be waived by the FBI in its sole discretion.

(w) Exemptions from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative interest in the individual by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and defuse any potential acts of terrorism or other potential violations of criminal law. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during an investigation and to take measures to impede the investigation, e.g., destroy evidence or flee the area to avoid the investigation.

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the access to accounting of disclosures provision of subsection (c)(3). The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of records, it will share that information in appropriate cases.

(3) From subsection (d)(1), (2), (3), and (4), (e)(4)(G) and (H) because these provisions concern individual access to and amendment of law enforcement, intelligence and counterintelligence, and counterterrorism records, and compliance could alert the subject of an authorized law enforcement or intelligence activity about that particular activity and the investigative interest of the FBI and/or other law enforcement or intelligence agencies. Providing access could compromise sensitive information classified to protect national security; disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; could provide information that would allow a subject to avoid detection or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, and witnesses.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes, and a major tenet of DIVS is that the relevance and utility of certain information that may have a nexus to terrorism or other crimes may not always be evident until and unless it is vetted and matched with other sources of information that are necessarily and lawfully maintained by the FBI.

(5) From subsection (e)(2) and (3) because application of this provision could present a serious impediment to efforts to solve crimes and improve national security. Application of these provisions would put the subject of an investigation on notice of that fact and allow the subject an opportunity to engage in conduct intended to impede that activity or avoid apprehension.
(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the Federal Register. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI. Further, greater specificity of properly classified records could compromise national security.

(7) From subsection (e)(5) because in the collection of information for authorized law enforcement and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. With time, seemingly irrelevant or untimely information may acquire new significance when new details are brought to light. Additionally, the information may aid in establishing patterns of activity and providing criminal or intelligence leads. It could impede investigative progress if it were necessary to assure relevance, accuracy, timeliness and completeness of all information obtained during the scope of an investigation. Further, some of the records searched by and/or contained in DIVS may come from other agencies and it would be administratively impossible for the FBI to vouch for the compliance of these agencies with this provision.

(8) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the FBI and may alert the subjects of law enforcement investigations, who might be otherwise unaware, to the fact of those investigations.

(9) From subsections (f) and (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:
[Order No. 40-80, 45 FR 5301, Jan. 23, 1980]

Editorial Note:
For Federal Register citations affecting § 16.96, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at www.fdsys.gov.
28 CFR Section 16.97: Exemption of Bureau of Prisons Systems—limited access.

(a) The following systems of records are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (H), (e)(8), (f) and (g):

2. Industrial Inmate Employment Record System (JUSTICE/BOP-003).
4. Inmate Central Record System (JUSTICE/BOP-005).
5. Inmate Commissary Accounts Record System (JUSTICE/BOP-006).
6. Inmate Physical and Mental Health Record System (JUSTICE/BOP-007).
7. Inmate Safety and Accident Compensation Record System (JUSTICE/BOP-008).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j).

(b) Exemptions from the particular subsections are justified for the following reasons:

1. From subsection (c)(3) because inmates will not be permitted to gain access or to contest contents of these record systems under the provisions of subsection (d) of 5 U.S.C. 552a. Revealing disclosure accountings can compromise legitimate law enforcement activities and Bureau of Prisons responsibilities.

2. From subsection (c)(4) because exemption from provisions of subsection (d) will make notification of formal disputes inapplicable.

3. From subsection (d) because exemption from this subsection is essential to protect internal processes by which Bureau personnel are able to formulate decisions and policies with regard to federal prisoners, to prevent disclosure of information to federal inmates that would jeopardize legitimate correctional interests of security, custody, or rehabilitation, and to permit receipt
of relevant information from other federal agencies, state and local law enforcement agencies, and federal and state probation and judicial offices.

(4) From subsection (e)(2) because primary collection of information directly from federal inmates about criminal sentences or criminal records is highly impractical and inappropriate.

(5) From subsection (e)(3) because in view of the Bureau of Prisons' responsibilities, application of this provision to its operations and collection of information is inappropriate.

(6) From subsection (e)(4)(H) because exemption from provisions of subsection (d) will make publication of agency procedures under this subsection inapplicable.

(7) From subsection (e)(8) because the nature of Bureau of Prisons law enforcement activities renders notice of compliance with compulsory legal process impractical.

(8) From subsection (f) because exemption from provisions of subsection (d) will render compliance with provisions of this subsection inapplicable.

(9) From subsection (g) because exemption from provisions of subsection (d) will render provisions of this subsection inapplicable.

(c) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(5) and (e)(8), and (g). In addition, the following system of records is exempted pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d), and (e)(1):


(d) These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g. public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(3) for similar reasons as those enumerated in paragraph (3).
(2) From subsection (c)(4) to the extent that exemption from subsection (d) will make notification of corrections or notations of disputes inapplicable.

(3) From the access provisions of subsection (d) to the extent that exemption from this subsection may appear to be necessary to prevent access by record subjects to information that may jeopardize the legitimate correctional interests of safety, security, and good order of Bureau of Prisons facilities; to protect the privacy of third parties; and to protect access to relevant information received from third parties, such as other Federal State, local and foreign law enforcement agencies, Federal and State probation and judicial offices, the disclosure of which may permit a record subject to evade apprehension, prosecution, etc.; and/or to otherwise protect investigatory or law enforcement information, whether received from other third parties, or whether developed internally by the BOP.

(4) From the amendment provisions of subsection (d) because amendment of the records would interfere with law enforcement operations and impose an impossible administrative burden. In addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that law enforcement and investigatory information be continuously reexamined, even where the information may have been collected from the record subject. Also, where records are provided by other Federal criminal justice agencies or other State, local and foreign jurisdictions, it may be administratively impossible to ensure compliance with this provision.

(5) From subsection (e)(1) to the extent that the BOP may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

(6) From subsection (e)(2) because primary collection of information directly from the record subject is often highly impractical, inappropriate and could result in inaccurate information.

(7) From subsection (e)(3) because compliance with this subsection may impede the collection of information that may be valuable to law enforcement interests.

(8) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance as an investigation progresses or with the passage of time, and could be relevant to future law enforcement decisions.
(9) From subsection (e)(8) because the nature of BOP law enforcement activities renders notice of compliance with compulsory legal process impractical and could seriously jeopardize institution security and personal safety and/or impede overall law enforcement efforts.

(10) From subsection (g) to the extent that the system is exempted from subsection (d).

(e) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(5) and (e)(8), (f) and (g):

Source: Telephone Activity Record System (JUSTICE/BOP-011).

(f) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) to the extent that this system of records is exempt from subsection (d), and for such reasons as those cited for subsection (d) in paragraph (f)(3) below.

(2) From subsection (c)(4) to the extent that exemption from subsection (d) makes this exemption inapplicable.

(3) From the access provisions of subsection (d) because exemption from this subsection is essential to prevent access of information by record subjects that may invade third party privacy; frustrate the investigative process; jeopardize the legitimate correctional interests of safety, security, and good order to prison facilities; or otherwise compromise, impede, or interfere with BOP or other law enforcement agency activities.

(4) From the amendment provisions from subsection (d) because amendment of the records may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that, in addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that law enforcement information be continuously reexamined, even where the information may have been collected from the record subject. Also, some of these records come from other Federal criminal justice agencies or State, local and foreign jurisdictions, or from Federal and State probation and judicial
offices, and it is administratively impossible to ensure that the records comply with this provision.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since it may result in inaccurate information.

(6) From subsection (e)(3) because in view of BOP's operational responsibilities, application of this provision to the collection of information is inappropriate. Application of this provision could provide the subject with substantial information which may in fact impede the information gathering process or compromise an investigation.

(7) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Material which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance at a later date or as an investigation progresses. Also, some of these records may come from other Federal, State, local and foreign law enforcement agencies, and from Federal and State probation and judicial offices and it is administratively impossible to ensure that the records comply with this provision. It would also require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject.

(8) From subsection (e)(8) because the nature of BOP law enforcement activities renders impractical the notice of compliance with compulsory legal process. This requirement could present a serious impediment to law enforcement such as revealing investigative techniques or the existence of confidential investigations, jeopardize the security of third parties, or otherwise compromise law enforcement efforts.

(9)-(10) [Reserved]

(11) From subsections (f) and (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(g) The following system of records is exempt pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2), and (3), (e)(5) and (e)(8), and (g) of 5 U.S.C. 552a. In addition, the following system of records
is exempt pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) of 5 U.S.C. 552a:

Source: Bureau of Prisons, Office of Internal Affairs Investigative Records, JUSTICE/BOP-012

(h) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the Office of Internal Affairs (OIA). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation, and reveal investigative interest by not only the OIA but also by the recipient agency. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation, release could result in activities that would impede or compromise law enforcement such as: the destruction of documentary evidence; improper influencing of witnesses; endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel; fabrication of testimony; and flight of the subject from the area. In addition, release of disclosure accounting could result in the release of properly classified information which could compromise the national defense or disrupt foreign policy.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could provide the subject of an investigation with information concerning law enforcement activities such as that relating to an actual or potential criminal, civil or regulatory violation; the existence of an investigation; the nature and scope of the information and evidence obtained as to his activities; the identity of confidential sources, witnesses, and law enforcement personnel; and information that may enable the subject to avoid detection or apprehension. Such disclosure would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation; endanger the physical safety of confidential sources, witnesses, and law enforcement personnel; and/or lead to the improper influencing of witnesses, the destruction of evidence, or the
fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which could compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIA for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIA may obtain information concerning actual or potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIA should retain this information as it may aid in establishing patterns of criminal activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation, information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may relate also to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(5) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a
subject's illegal acts, violations of rules of conduct, or any other misconduct must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

(6) From subsection (e)(3) because the application of this provision would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5) because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Material which may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance as an investigation progresses. The restrictions of this provision could interfere with the preparation of a complete investigation report, and thereby impede effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigation techniques, procedures, and/or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), and (k)(2) of the Privacy Act.

(i) Consistent with the legislative purpose of the Privacy Act of 1974 (Pub. L. 93-579) the BOP has initiated a procedure whereby federal inmates in custody may gain access and review their individual prison files maintained at the institution of incarceration. Access to these files will be limited only to the extent that the disclosure of records to the inmate would jeopardize internal decision-making or policy determinations essential to the effective operation of the Bureau of Prisons; to the extent that disclosure of the records to the inmate would jeopardize privacy rights of others, or a legitimate correctional interest of security, custody, or rehabilitation; and to the extent information is furnished with a legitimate expectation of confidentiality. The Bureau of Prisons will continue to provide access to former inmates under existing regulations as is consistent with the interests listed above. Under present Bureau of Prisons
regulations, inmates in federal institutions may file administrative complaints on any subject under the control of the Bureau. This would include complaints pertaining to information contained in these systems of records.

(j) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Central Records System, (Justice/BOP-005).

(k) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g. public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

1. From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

2. From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance during the course of an investigation or with the passage of time, and could be relevant to future law enforcement decisions. In addition, because many of these records come from the courts and other state and local criminal justice agencies, it is administratively impossible for them and the Bureau to ensure compliance with this provision. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the safety and security of the prisons and the public.

(l) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Trust Fund Accounts and Commissary Record System, (Justice/BOP-006).

(m) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the
information collected, e.g. public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

(2) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance as an investigation progresses or with the passage of time, and could be relevant to future law enforcement decisions. In addition, amendment of the records may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that law enforcement information be continuously reexamined, even where the information may have been collected from the record subject or other criminal justice agencies. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the safety and security of the prisons and the public.

(n) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Physical and Mental Health Records System, (Justice/BOP-007).

(o) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g. public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.
(2) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance during the course of an investigation or with the passage of time, and could be relevant to future law enforcement decisions. In addition, because many of these records come from sources outside the Bureau of Prisons, it is administratively impossible for them and the Bureau to ensure compliance with this provision. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the health care of the inmates and the safety and security of the prisons and the public.

(p) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4), (d)(1)-(4), (e)(2) and (3), (e)(5), and (g):

Inmate Electronic Message Record System (JUSTICE /BOP-013).

(q) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) to the extent that this system of records is exempt from subsection (d), and for such reasons as those cited for subsection (d) in paragraph (q)(3) below.

(2) From subsection (c)(4) to the extent that exemption from subsection (d) makes this exemption inapplicable.

(3) From the access provisions of subsection (d) because exemption from this subsection is essential to prevent access of information by record subjects that may invade third party privacy; frustrate the investigative process; jeopardize the legitimate correctional interests of safety, security and good order to prison facilities; or otherwise compromise, impede, or interfere with BOP or other law enforcement agency activities.

(4) From the amendment provisions of subsection (d) because amendment of the records may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that, in addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that
law enforcement information be continuously reexamined, even where the information may have been collected from the record subject. Also, some of these records come from other Federal criminal justice agencies or State, local and foreign jurisdictions, or from Federal and State probation and judicial offices, and it is administratively impossible to ensure that records comply with this provision.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since it may result in inaccurate information and compromise ongoing criminal investigations or correctional management decisions.

(6) From subsection (e)(3) because in view of BOP's operational responsibilities, application of this provision to the collection of information is inappropriate. Application of this provision could provide the subject with substantial information which may in fact impede the information gathering process or compromise ongoing criminal investigations or correctional management decisions.

(7) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Material which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance at a later date or as an investigation progresses. Also, some of these records may come from other Federal, State, local and foreign law enforcement agencies, and from Federal and State probation and judicial offices and it is administratively impossible to ensure that the records comply with this provision. It would also require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject.

(8) From subsection (g) to the extent that this system is exempted from other provisions of the Act.

Official Citation:
[Order No. 645-76, 41 FR 12640, Mar. 26, 1976]

Editorial Note:
For Federal Register citations affecting § 16.97, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at www.fdsys.gov.
28 CFR Section 16.98: Exemption of the Drug Enforcement Administration (DEA)—limited access.

(a) The following systems of records are exempt from 5 U.S.C. 552a(c)(3) and (d):

   (1) Automated Records and Consummated Orders System/Diversion Analysis and Detection System (ARCOS/DADS) (Justice/DEA-003)

   (2) Controlled Substances Act Registration Records (Justice/DEA-005)

   (3) Registration Status/Investigatory Records (Justice/DEA-012)

(b) These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Exemptions from the particular subsections are justified for the following reasons:

   (1) From subsection (c)(3) because release of the disclosure accounting would enable the subject of an investigation to gain valuable information concerning the nature and scope of the investigation and seriously hamper the regulatory functions of the DEA.

   (2) From subsection (d) because access to records contained in these systems may provide the subject of an investigation information that could enable him to avoid compliance with the Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513).

(c) Systems of records identified in paragraphs (c)(1) through (c)(7) below are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d)(1), (2). (3) and (4); (e)(1), (2) and (3), (e)(5), (e)(8); and (g) of 5 U.S.C. 552a. In addition, systems of records identified in paragraphs (c)(1), (c)(2), (c)(3), (c)(4), (c)(5), and (c)(6) below are also exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) from subsections (c)(3); (d)(1), (2), (3) and (4); and (e)(1):

   (1) Air Intelligence Program (Justice/DEA-001)

   (2) Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002)

   (3) Investigative Reporting and Filing System (Justice/DEA-008)

   (4) Planning and Inspection Division Records (Justice/DEA-010)

   (5) Operation Files (Justice/DEA-011)

   (6) Security Files (Justice/DEA-013)
(7) System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014)

(d) Exemptions apply to the following systems of records only to the extent that information in the systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2): Air Intelligence Program (Justice/DEA-001); Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002); Planning and Inspection Division Records (Justice/DEA-010); and Security Files (Justice/DEA-013). Exemptions apply to the Investigative Reporting and Filing System (Justice/DEA-008) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) (2) and (k)(1). Exemptions apply to the Operations Files (Justice/DEA-011) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Exemptions apply to the System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Exemption from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting would provide to the subjects of an investigation significant information concerning the nature of the investigation and thus would present the same impediments to law enforcement as those enumerated in paragraph (d)(3) regarding exemption from subsection (d).

(2) From subsection (c)(4) to the extent that it is not applicable because an exemption is being claimed from subsection (d).

(3) From the access provisions of subsection (d) because access to records in this system of records would present a serious impediment to law enforcement. Specifically, it could inform the record subject of an actual or potential criminal, civil, or regulatory investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. Similarly, it may alert collateral suspects yet unprosecuted in closed cases. It could prevent the successful completion of the investigation; endanger the life, health, or physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony; or it may simply reveal a sensitive investigative technique. In addition, granting access to such information could result in the disclosure of confidential/security-sensitive or other information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. From the
amendment provisions of subsection (d) because amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the DEA for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations during which DEA may obtain properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the DEA's investigative activities DEA may detect the violation of either drug-related or non-drug related laws. In the interests of effective law enforcement, it is necessary that DEA retain all information obtained because it can aid in establishing patterns of activity and provide valuable leads for Federal and other law enforcement agencies or otherwise assist such agencies in discharging their law enforcement responsibilities. Such information may include properly classified information, the retention of which could be in the interests of national defense and/or foreign policy.

(5) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful prosecution.

(6) From subsection (e)(3) because the requirements thereof would constitute a serious impediment to law enforcement in that they could compromise the existence of an actual or potential confidential investigation
and/or permit the record subject to speculate on the identity of a potential confidential source, and endanger the life, health or physical safety or either actual or potential confidential informants and witnesses, and of investigators/law enforcement personnel. In addition, the notification requirement of subsection (e)(3) could impede collection of that information from the record subject, making it necessary to collect the information solely from third party sources and thereby inhibiting law enforcement efforts.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1) and (k)(2) of the Privacy Act.

(e) The following systems of records are exempt from 5 U.S.C. 552a (d)(1) and (e)(1):

(1) Grants of Confidentiality Files (GCF) (Justice/DEA-017), and

(2) DEA Applicant Investigations (Justice/DEA-018).

(f) These exemptions apply only to the extent that information in these systems is subject to exception pursuant to 5 U.S.C. 552a(k)(5). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a grant of confidentiality with DEA. By permitting access to information which may reveal the identity of the source of that information—after a promise of confidentiality has been given—DEA would breach the promised confidentiality. Ultimately, such breaches would restrict the free flow of information which is vital to a determination of an applicant's qualifications for a grant.
(2) From subsection (e)(1) because in the collection of information for investigative and evaluation purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other apparently irrelevant information, can on occasion provide a composite picture of an applicant which assists in determining whether a grant of confidentiality is warranted.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g): El Paso Intelligence Center (EPIC) Seizure System (ESS) (JUSTICE/DEA-022). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement and counter-drug purposes of this system, and the overall law enforcement process, the applicable exemption may be waived by the DEA in its sole discretion.

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would potentially reveal any investigative interest in the individual. Revealing this information would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants. Similarly, disclosing this information could reasonably be expected to compromise ongoing investigatory efforts by notifying the record subject that he/she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of records contained in this system, which consists of counter-drug and criminal investigatory records. Compliance with these provisions could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension.
These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation; endanger the physical safety of witnesses or informants; or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary to complete an identity comparison between the individual being screened and a known or suspected criminal or terrorist. Also, it may not always be known what information will be relevant to law enforcement for the purpose of conducting an operational response or on-going investigation.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to law enforcement and counter-drug efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counter-drug investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) because the requirements thereof would constitute a serious impediment to law enforcement in that they could compromise the existence of an actual or potential confidential investigation and/or permit the record subject to speculate on the identity of a potential confidential source, and endanger the life, health or physical safety of either actual or potential confidential informants and witnesses, and of investigators/law enforcement personnel. In addition, the notification requirement of subsection (e)(3) could impede collection of that information from the record subject, making it necessary to collect the information solely from third party sources and thereby inhibiting law enforcement efforts.

(7) From subsection (e)(5) because many of the records in this system are derived from other domestic record systems and therefore it is not possible for the DEA and EPIC to vouch for their compliance with this provision. In addition, EPIC supports but does not conduct investigations; therefore, it must be able to collect information related to illegal drug and other criminal activities and encounters for distribution to law enforcement and intelligence agencies that do conduct counter-drug investigations. In the collection of information for law enforcement and counter-drug purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by
(e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. EPIC has, however, implemented internal quality assurance procedures to ensure that ESS data is as thorough, accurate, and current as possible. ESS is also exempt from the requirements of subsection (e)(5) in order to prevent the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the ESS. ESS records are exempt from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of investigations. Exempting ESS from subsection (e)(5) serves to prevent the assertion of challenges to a record's accuracy, timeliness, completeness, and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the DEA and EPIC and could alert the subjects of counter-drug, counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known. Additionally, compliance could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:


(a) The following systems of records of the Immigration and Naturalization Service are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e)(1), (2) and (3), (e) (4)(G) and (H), (e) (5) and (8), and (g):

(1) The Immigration and Naturalization Service Alien File (A-File) and Central Index System (CIS), JUSTICE/INS-001A.

(2) The Immigration and Naturalization Service Index System, JUSTICE/INS-001 which consists of the following subsystems:
(i) Agency Information Control Record Index.

(ii) Alien Enemy Index.

(iii) Congressional Mail Unit Index.

(iv) Air Detail Office Index.

(v) Anti-smuggling Index (general).

(vi) Anti-smuggling Information Centers Systems for Canadian and Mexican Borders.

(vii) Border Patrol Sectors General Index System.

(viii) Contact Index.

(ix) Criminal, Narcotic, Racketeer and Subversive Indexes.

(x) Enforcement Correspondence Control Index System.

(xi) Document Vendors and Alterers Index.

(xii) Informant Index.

(xiii) Suspect Third Party Index.

(xiv) Examination Correspondence Control Index.

(xv) Extension Training Enrollee Index.

(xvi) Intelligence Index.

(xvii) Naturalization and Citizenship Indexes.

(xviii) Personnel Investigations Unit Indexes.

(xix) Service Look-Out Subsystem.

(xx) White House and Attorney General Correspondence Control Index.

(xxi) Fraudulent Document Center Index.

(xxii) Emergency Reassignment Index.

(xxiii) Alien Documentation, Identification, and Telecommunication (ADIT) System.
The exemptions apply to the extent that information in these subsystems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(3) The Immigration and Naturalization Service “National Automated Immigration Lookout System (NAILS) JUSTICE/INS-032.” The exemptions apply only to the extent that records in the system are subject to exemptions pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosure pursuant to the routine uses published for these subsystems would permit the subject of a criminal or civil investigation to obtain valuable information concerning the nature of that investigation and present a serious impediment to law enforcement.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in these subsystems would inform the subject of a criminal or civil investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and present a serious impediment to law enforcement.

(4) From subsection (e)(1) because in the course of criminal or civil investigations, the Immigration and Naturalization Service often obtains information concerning the violation of laws other than those relating to violations over which INS has investigative jurisdiction. In the interests of effective law enforcement, it is necessary that INS retain this information since it can aid in establishing patterns of criminal activity and provide valuable leads for those law enforcement agencies that are charged with enforcing other segments of the criminal law.

(5) From subsection (e)(2) because in a criminal or civil investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the
identity of confidential sources of information and endanger the life or physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because these subsystems of records are exempt from individual access pursuant to subsection (j) of the Privacy Act of 1974.

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the Immigration and Naturalization Service's ability to issue administrative subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (g) because these subsystems of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(11) In addition, these systems of records are exempt from subsections (c)(3), (d), (e)(1), (e)(4) (G) and (H) to the extent they are subject to exemption pursuant to 5 U.S.C. 552a(k)(1). To permit access to records classified pursuant to Executive Order would violate the Executive Order protecting classified information.

(c) The Border Patrol Academy Index Subsystem is exempt from 5 U.S.C. 552a (d) and (f).

This exemption applies only to the extent that information in this subsystem is subject to exemption pursuant to 5 U.S.C. 552a(k).

(d) Exemptions for the particular subsections are justified for the following reasons.

(1) From subsection (d) because exemption is claimed only for those testing and examination materials used to determine an individual's qualifications for retention and promotion in the Immigration and Naturalization Service.
Service. This is necessary to protect the integrity of testing materials and to insure fair and uniform examinations.

(2) From subsection (f) because the subsystem of records has been exempted from the access provisions of subsection (d).

(e) The Orphan Petitioner Index and Files (Justice/INS-007) system of records is exempt from 5 U.S.C. 552a(d). This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

(f) Exemption from paragraph (d) of this section is claimed solely because of the possibility of receipt of classified information during the course of INS investigation of prospective adoptive parents.

Although it would be rare, prospective adoptive parents may originally be from foreign countries (for example) and information received on them from their native countries may require classification under Executive Order 12356 which safeguards national security information. If such information is relevant to the INS determination with respect to adoption, the information would be kept in the file and would be classified accordingly. Therefore, access could not be granted to the record subject under the Privacy Act without violating E.O. 12356.

(g) The Office of Internal Audit Investigations Index and Records (Justice/INS-002) system of records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5) and (8); and (g), but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in the system are subject to exemption therefrom. In addition, this system of records is also exempt under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in the system are subject to exemption therefrom.

(h) The following justification apply to the exemptions from particular subsections:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosure could permit the subject of an actual or potential criminal or civil investigation to obtain valuable information concerning the existence and nature of the investigation, the fact that individuals are subjects of the investigation, and present a serious impediment to law enforcement.

(2) From subsection (c)(4) to the extent that the exemption from subsection (d) is applicable. Subsection (c)(4) will not be applicable to the extent that records in the system are properly withholdable under subsection (d).
(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of a criminal or civil investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to their activities; of the identity of confidential sources, witnesses and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. Such disclosures would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation; endanger the physical safety of confidential sources, witnesses, and law enforcement personnel; and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to these records could result in a disclosure that would constitute an unwarranted invasion of the privacy of third parties. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because in the course of criminal or civil investigations, the Immigration and Naturalization Service often obtains information concerning the violation of laws other than those relating to violations over which INS has investigative jurisdiction, in the interests of effective law enforcement, it is necessary that INS retain this information since it can aid in establishing patterns of criminal activity and provide valuable leads for those law enforcement agencies that are charged with enforcing other segments of the criminal law.

(5) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment of criminal law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life or physical safety of confidential informants.

(7) From subsection (e)(5) because in the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of
subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to criminal law enforcement as this could interfere with the Immigration and Naturalization Service’s ability to issue administrative subpoenas and could reveal investigative techniques and procedures.

(9) From subsection (g) for those portions of this system of records that were compiled for criminal law enforcement purposes and which are subject to exemption from the access provisions of subsections (d) pursuant to subsection (j)(2).

(i) The Law Enforcement Support Center Database (LESC) (Justice/INS-023) system of records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4); (d); (e)(1), (2), (3), (5), (8) and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in the system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in the system are subject to exemption therefrom.

(j) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of a criminal or civil investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to their activities; and of information that may enable the subject to avoid detection or apprehension. Such disclosures would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation or other law enforcement operation such as deportation or exclusion. In addition, granting access to these records could result in a
disclosure that would constitute an unwarranted invasion of the privacy of third parties. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to criminal law enforcement in that it could compromise the existence of a confidential investigation.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(k) The Attorney/Representative Complaint/Petition File (JUSTICE/INS-022) system of records is exempt under the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5), and (8); and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in this system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a (k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in this system are subject to exemption therefrom.

(l) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.
(3) From the access and amendment provisions of subsection (d) for reasons stated in paragraph (h)(3) of this section.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) for reasons stated in paragraph (h)(6) of this section.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

(m) The Worksite Enforcement Activity and Records Index (LYNX) (JUSTICE/INS-025) system of records is exempt under the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5), and (8); and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in this system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in this system are subject to exemption therefrom.

(n) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons started in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) for reasons sated in paragraph (h)(3) of this section.
(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) for reasons stated in paragraph (h)(6) of this section.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

Official Citation:

28 CFR Section 16.100: Exemption of Office of Justice Programs—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) The Civil Rights Investigative System (JUSTICE/OJP-008).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(b) Exemption from subsection (d) is claimed since access to information in the Civil Rights Investigative System prior to final administrative resolution will deter conciliation and compliance efforts. Consistent with the legislative purpose of the Privacy Act of 1974, decisions to release information from the system will be made on a case-by-case basis and information will be made available where it does not compromise the complaint and compliance process. In addition, where explicit promises of confidentiality must be made to a source during an
investigation, disclosure will be limited to the extent that the identity of such confidential sources will not be compromised.

**Official Citation:**

28 CFR Section 16.101: Exemption of U.S. Marshals Service Systems—limited access, as indicated.

(a) The following system of records is exempt from 5 U.S.C. 552(a)(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) Warrant Information System (JUSTICE/USM-007).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of disclosure accounting for disclosure made pursuant to subsection (b) of the Act, including those permitted under routine uses published for this system of records would permit a person to determine whether he is the subject of a criminal investigation, and to determine whether a warrant has been issued against him, and therefore present a serious impediment to law enforcement.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d) of the Act, this section is inapplicable.

(3) From subsection (d) because access to records would inform a person for whom a federal warrant has been issued of the nature and scope of information obtained as to his activities, of the identity of informants, and afford the person sufficient information to enable the subject to avoid apprehension. These factors would present a serious impediment to law enforcement in that they would thwart the warrant process and endanger lives of informants etc.

(4) From subsections (e)(1) and (e)(5) because the requirements of these subsections would present a serious impediment to law enforcement in that it is impossible to determine in advance what information collected during an
In the interest of effective law enforcement, it is appropriate in a thorough investigation to retain seemingly irrelevant, untimely, or inaccurate information which, with the passage of time, would aid in establishing patterns of activity and provide investigative leads toward fugitive apprehension and assist in law enforcement activities of other agencies.

(5) From subsection (e)(2) because the requirement that information be collected to the greatest extent practical from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the warrant and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal identity of confidential informants.

(7) From subsections (e)(4) (G) and (H) since an exemption is being claimed for subsections (f) and (d) of the Act, these subsections are inapplicable.

(8) From subsection (e)(8) because the individual notice requirement of this subsection would present a serious impediment to law enforcement in that it would give persons sufficient warning to avoid warrants, subpoena, etc.

(9) From subsection (f) because procedures for notice to an individual pursuant to subsection (f)(1) as to existence of records pertaining to him dealing with warrants must be exempted because such notice to individuals would be detrimental to the successful service of a warrant. Since an exemption is being claimed for subsection (d) of the Act the rules required pursuant to subsections (f) (2) through (5) are inapplicable to this system of records.

(10) From subsection (g) since an exemption is being claimed for subsection (d) and (f) this section is inapplicable and is exempted for the reasons set forth for these subsections.

(c) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e)(8), (f)(2) and (g):


These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).
(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act including those permitted under routine uses published for this system of records would hamper the effective functioning of the Witness Security Program which by its very nature requires strict confidentiality vis-a-vis the records.

(2) From subsection (c)(4) for the reason stated in (b)(2) of this section.

(3) From subsection (d) because the U.S. Marshals Service Witness Security Program aids efforts of law enforcement officials to prevent, control or reduce crime. Access to records would present a serious impediment to effective law enforcement through revelation of confidential sources and through disclosure of operating procedures of the program, and through increased exposure of the program to the public.

(4) From subsection (e)(2) because in the Witness Security Program the requirement that information be collected to the greatest extent possible from the subject individual would constitute an impediment to the program, which is sometimes dependent on sources other than the subject witness for verification of information pertaining to the witness.

(5) From subsection (e)(3) for the reason stated in (b)(6) of this section.

(6) From subsection (e)(4) (G) and (H) for the reason stated in (b)(7) of this section.

(7) From subsection (e)(8) for the reason stated in (b)(8) of this section.

(8) From subsection (f)(2) since an exemption is being claimed for subsection (d) of the Act the rules required pursuant to subsection (f) (2) through (5) are inapplicable to this system of records.

(9) From subsection (g) for the reason stated in (b)(10) of this section.

(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g).

(1) Internal Affairs System (JUSTICE/USM-002)—Limited access. These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2) or (k)(5). Where compliance would not interfere with or adversely affect the law enforcement process, the USMS may waive the exemptions, either partially or totally.
(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3) and (d) to the extent that release of the disclosure accounting may impede or interfere with civil or criminal law enforcement efforts, reveal a source who furnished information to the Government in confidence, and/or result in an unwarranted invasion of the personal privacy of collateral record subjects or other third party individuals.

(2) From subsection (c)(4) for the reason stated in (b)(2) of this section.

(3) From subsection (e)(1) to the extent that it is necessary to retain all information in order not to impede, compromise, or interfere with civil or criminal law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law agencies in discharging their law enforcement responsibilities.

(4) From subsection (e)(2) because the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to compromise the investigation and avoid detection or apprehension.

(5) From subsection (e)(3) for the reason stated in (b)(6) of this section.

(6) From subsections (e)(4) (G) and (H) for the reason stated in (b)(7) of this section.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes and interfere with the preparation of a complete investigative report or otherwise impede effective law enforcement.

(8) From subsection (e)(8) because the individual notice requirement of this subsection would present a serious impediment to law enforcement in that the subject of the investigation would be alerted as to the existence of the investigation and therefore be able to compromise the investigation and avoid detection, subpoena, etc.
(9) From subsection (f) because procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records dealing with investigations of criminal or civil law violations would enable the individual to compromise the investigation and evade detection or apprehension. Since an exemption is being claimed for subsection (d) of the Act, the rules required pursuant to subsections (f)(2) through (f)(5) are not applicable to this system.

(10) From subsection (g) for the reason stated in (b)(10) of this section.

(g) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) U.S. Marshals Service Threat Analysis Information System (JUSTICE/USM-009).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit a person to determine whether he or she has been identified as a specific threat to USMS protectees and to determine the need for countermeasures to USMS protective activities and thereby present a serious impediment to law enforcement.

(2) From subsection (c)(4) because it is inapplicable since an exemption is being claimed for subsection (d).

(3) From subsection (d) because to permit access to records would inform a person of the nature and scope of information obtained as to his or her threat-related activities and of the identity of confidential sources, and afford the person sufficient information to develop countermeasures to thwart protective arrangements and endanger lives of USMS protectees, informants, etc. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because the collection of investigatory information used to assess the existence, extent and likelihood of a threat situation necessarily includes material from which it is impossible to identify and segregate information which may not be important to the conduct of a thorough assessment. It is often impossible to determine in advance if all information
collected is accurate, relevant, timely and complete but, in the interests of developing effective protective measures, it is necessary that the U.S. Marshals Service retain this information in order to establish patterns of activity to aid in accurately assessing threat situations. The restrictions of subsections (e)(1) and (5) would impede the protective responsibilities of the Service and could result in death or serious injury to Marshals Service protectees.

(5) From subsection (e)(2) because to collect information from the subject individual would serve notice that he or she is identified as a specific threat to USMS protectees and would enable the subject individual to develop countermeasures to protective activities and thereby present a serious impediment to law enforcement.

(6) From subsection (e)(3) because to inform individuals as required by this subsection would enable the subject individual to develop countermeasures to USMS protective arrangements or identify confidential sources and thereby present a serious impediment to law enforcement.

(7) From subsections (e)(4) (G) and (H) because they are inapplicable since an exemption is being claimed for subsections (d) and (f) of the Act.

(8) From subsection (e)(8) because to serve notice would give persons sufficient warning to develop countermeasures to protective arrangements and thereby present a serious impediment to law enforcement through compromise of protective procedures, etc.

(9) From subsection (f) because this system of records is exempt from the provisions of subsection (d).

(10) From subsection (g) because it is inapplicable since an exemption is being claimed for subsections (d) and (f).

(i) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (d):

(1) Judicial Facility Security Index System (JUSTICE/USM-010)

These exemptions apply only to the extent that information in this system is exempt pursuant to 5 U.S.C. 552a(k)(5).

(j) Exemptions from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3) only to the extent that release of the disclosure accounting would reveal the identity of a confidential source.

(2) From subsection (d) only to the extent that access to information would reveal the identity of a confidential source.

(k) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) U.S. Marshals Service Freedom of Information/Privacy Act (FOIA/PA) Files (JUSTICE/USM-012).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(2) and (k)(5).

(l) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the existence and nature of the investigation and present a serious impediment to law enforcement.

(2) From subsection (c)(4) because that portion of this system which consists of investigatory records compiled for law enforcement purposes is being exempted from the provisions of subsection (d), rendering this provision not applicable.

(3) From subsection (d) because to permit access to investigatory records would reveal the identity of confidential sources and impede ongoing investigative or law enforcement activities by the premature disclosure of information related to those efforts. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because it is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide leads in criminal investigations.

(5) From subsection (e)(2) because to collect information from the subject individual would serve notice that he or she is the subject of criminal
investigative or law enforcement activity and thereby present a serious impediment to law enforcement.

(6) From subsection (e)(3) because to inform individuals as required by this subsection would enable the subject individual to identify confidential sources, reveal the existence of an investigation, and compromise law enforcement efforts.

(7) From subsections (e)(4) (G) and (H) because they are inapplicable since an exemption is being claimed for subsections (d) and (f) for investigatory records contained in this system.

(8) From subsection (e)(8) because to serve notice would give persons sufficient warning to evade law enforcement efforts.

(9) From subsection (f) because investigatory records contained in this system are exempt from the provisions of subsection (d).

(10) From subsection (g) because it is inapplicable since an exemption is being claimed for subsections (d) and (f).

(m) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e)(8), (f) and (g):

(1) U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files (JUSTICE/USM-013).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(5).

(n) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting for disclosures pursuant to the routine uses published for this system would permit the subject of a criminal or civil case or matter under investigation, or a case or matter in litigation, or under regulatory or administrative review or action, to obtain valuable information concerning the nature of that investigation, case or matter, and present a serious impediment to law enforcement or civil legal activities, or reveal a confidential source.

(2) From subsection (c)(4) because the exemption claimed for subsection (d) will make this section inapplicable.
(3) From subsection (d) because to permit access to records contained in this system would provide information concerning litigation strategy, or case development, and/or reveal the nature of the criminal or civil case or matter under investigation or administrative review, or in litigation, and present a serious impediment to law enforcement or civil legal activities, or reveal a confidential source.

(4) From subsection (e)(2) because effective legal representation, defense, or claim adjudication necessitates collecting information from all individuals having knowledge of the criminal or civil case or matter. To collect information primarily from the subject individual would present a serious impediment to law enforcement or civil legal activities.

(5) From subsection (e)(3) because to inform the individuals as required by this subsection would permit the subject of a criminal or civil matter under investigation or administrative review to compromise that investigation or administrative review and thereby impede law enforcement efforts or civil legal activities.

(6) From subsections (e)(4) (G) and (H) because these provisions are inapplicable since this system is exempt from subsections (d) and (f) of the Act.

(7) From subsection (e)(8) because to serve notice would give persons sufficient warning to compromise a criminal or civil investigation or administrative review and thereby impede law enforcement of civil legal activities.

(8) From subsection (f) because this system of records is exempt from the provisions of subsection (d).

(9) From subsection (g) because it is inapplicable since an exemption is claimed for subsections (d) and (f).

(o) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2), (5) and (g):

(1) U.S. Marshals Service Prisoner Transportation System (JUSTICE/USM-003).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(p) Exemptions from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3) where the release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act would reveal a source who furnished information to the Government in confidence.

(2) From subsection (c)(4) to the extent that the system is exempt from subsection (d).

(3) From subsection (d) because access to records would reveal the names and other information pertaining to prisoners, including sensitive security information such as the identities and locations of confidential sources, e.g., informants and protected witnesses; and disclose access codes, data entry codes and message routing symbols used in law enforcement communications systems to schedule and effect prisoner movements. Thus, such a compromise of law enforcement communications systems would subject law enforcement personnel and other prisoners to harassment and possible danger, and present a serious threat to law enforcement activities. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden by requiring that information affecting the prisoner's security classification be continuously reinvestigated when contested by the prisoner, or by anyone on his behalf.

(4) From subsections (e)(1) and (5) because the security classification of prisoners is based upon information collected during official criminal investigations; and, in the interest of ensuring safe and secure prisoner movements it may be necessary to retain information the relevance, necessity, accuracy, timeliness, and completeness of which cannot be readily established, but which may subsequently prove useful in establishing patterns of criminal activity or avoidance, and thus be essential to assigning an appropriate security classification to the prisoner. The restrictions of subsection (e)(1) and (5) would impede the information collection responsibilities of the USMS, and the lack of all available information could result in death or serious injury to USMS and other law enforcement personnel, prisoners in custody, and members of the public.

(5) From subsection (e)(2) because the requirement to collect information from the subject individual would impede the information collection responsibilities of the USMS in that the USMS is often dependent upon sources other than the subject individual for verification of information pertaining to security risks posed by the individual prisoner.

(6) From subsection (g) to the extent that the system is exempt from subsection (d).

(q) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2), (3), (e)(5) and (e)(8) and (g):
(1) U.S. Marshals Service Prisoner Processing and Population Management System (JUSTICE/USM-005).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(r) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit the subject of a criminal proceeding to determine the extent or nature of law enforcement authorities' knowledge regarding his/her alleged misconduct or criminal activities. The disclosure of such information could alert the subject to devise ways in which to conceal his/her activities and/or prevent law enforcement from learning additional information about his/her activities, or otherwise inhibit law enforcement efforts. In addition, where the individual is the subject of an ongoing or potential inquiry/investigation, such release could reveal the nature thereof prematurely, and may also enable the subject to determine the identity of witnesses and informants. Such disclosure could compromise the ongoing or potential inquiry/investigation, endanger the lives of witnesses and informants, or otherwise impede or thwart law enforcement efforts.

(2) From subsection (c)(4) to the extent that the system is exempt from subsection (d).

(3) From subsection (d) because to permit unlimited access would permit the subject of a criminal proceeding to determine the extent or nature of law enforcement authorities' knowledge regarding his/her alleged misconduct or criminal activities. The disclosure of such information could alert the subject to devise ways in which to conceal his/her activities and/or prevent law enforcement from learning additional information about his/her activities, or otherwise inhibit law enforcement efforts. Disclosure would also allow the subject to obtain sensitive information concerning the existence and nature of security measures and jeopardize the safe and secure transfer of the prisoner, the safety and security of other prisoners, informants and witnesses, law enforcement personnel, and the public. In addition, disclosure may enable the subject to learn prematurely of an ongoing or potential inquiry/investigation, and may also permit him/her to determine the identities of confidential sources, informants, or protected witnesses. Such disclosure could compromise the ongoing or potential inquiry/investigation, endanger the lives of witnesses and informants, or otherwise impede or thwart law enforcement efforts. Disclosure may also constitute an unwarranted invasion of the personal privacy of third parties. Further, disclosure would reveal access codes, data entry codes and message
routing symbols used in law enforcement communications systems. Access to such codes and symbols would permit the subject to impede the flow of law enforcement communications and compromise the integrity of law enforcement information, and thus present a serious threat to law enforcement activities. To permit amendment of the records would expose security matters, and would impose an impossible administrative burden by requiring that security precautions, and information pertaining thereto, be continuously reevaluated if contested by the prisoner, or by anyone on his or her behalf. Similarly, to permit amendment could interfere with ongoing or potential inquiries/investigations by requiring that such inquiries/investigations be continuously reinvestigated, or that information collected (the relevance and accuracy of which cannot readily be determined) be subjected to continuous change.

(4) From subsections (e)(1) and (5) because the system may contain investigatory information or information which is derived from information collected during official criminal investigations. In the interest of effective law enforcement and litigation, of securing the prisoner and of protecting the public, it may be necessary to retain information the relevance, necessity, accuracy, timeliness and completeness of which cannot be readily established. Such information may nevertheless provide investigative leads to other Federal or law enforcement agencies, or prove necessary to establish patterns of criminal activity or behavior, and/or prove essential to the safe and secure detention (and movement) of prisoners. Further, the provisions of (e)(1) and (e)(5) would restrict the ability of the USMS in exercising its judgment in reporting information during investigations or during the development of appropriate security measures, and thus present a serious impediment to law enforcement efforts.

(5) From subsection (e)(2) because the requirement to collect information from the subject individual would impede the information collection responsibilities of the USMS which is often dependent upon sources other than the subject individual for verification of information pertaining to security risks posed by the individual prisoner, to alleged misconduct or criminal activity of the prisoner, or to any matter affecting the safekeeping and disposition of the individual prisoner.

(6) From subsection (e)(3) because to inform individuals as required by this subsection could impede the information gathering process, reveal the existence of an ongoing or potential inquiry/investigation or security procedure, and compromise law enforcement efforts.

(7) From subsection (e)(8) because to serve notice would give persons sufficient warning to compromise an ongoing or potential inquiry/investigation and thereby evade and impede law enforcement and security efforts.
(8) From subsection (g) to the extent that the system is exempt from subsection (d).

The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2), (3), (e) (5) and (e) (8) and (g):

Joint Automated Booking Stations, Justice/USM-014

(t) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not interfere with or adversely affect the law enforcement process, the USMS may waive the exemptions, either partially or totally. Exemption from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3) and (d) to the extent that access to records in this system of records may impede or interfere with law enforcement efforts, result in the disclosure of information that would constitute and unwarranted invasion of the personal privacy of collateral record subjects or other third parties, and/or jeopardize the health and/or safety of third parties.

(2) Where access to certain records may be appropriate, exemption from the amendment provisions of subsection (d)(2) is necessary to the extent that the necessary and appropriate justification, together with proof of record inaccuracy, is not provided, and/or to the extent that numerous, frivolous requests to amend could impose an impossible administrative burden by requiring agencies to continuously review booking and arrest data, much of which is collected from the arrestee during the arrest.

(3) From subsection (e)(1) to the extent that it is necessary to retain all information in order not to impede, compromise, or interfere with law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law enforcement agencies in discharging their law enforcement responsibilities.

(4) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement since it may be necessary to obtain and verify information from a variety of sources other than the record subject to ensure safekeeping, security, and effective law enforcement. For example, it may be necessary that medical and psychiatric personnel provide information regarding the subject's behavior, physical health, or mental stability, etc. To ensure proper care while in custody, or it may be necessary to obtain information from a case agent or the court to ensure proper disposition of the subject individual.
(5) From subsection (e)(3) because the requirement that agencies inform each individual whom it asks to supply information of such information as is required by subsection (e)(3) may, in some cases, impede the information gathering process or otherwise interfere with or compromise law enforcement efforts, e.g., the subject may deliberately withhold information, or give erroneous information.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes and may prevent the eventual development of the necessary criminal intelligence or otherwise impede effective law enforcement.

(7) From subsection (e)(8) to the extent that such notice may impede, interfere with, or otherwise compromise law enforcement and security efforts.

(8) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(u) Consistent with the legislative purpose of the Privacy Act of 1974, the United States Marshals Service will grant access to nonexempt material in records which are maintained by the Service. Disclosure will be governed by the Department's Privacy Regulations, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal, civil or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

Official Citation:

(a) The following system of records is exempted pursuant to provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G), (H), and (I), (e)(5) and (8), (f), (g), and (h) of 5 U.S.C. 552a; in addition the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552 (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of 5 U.S.C. 552a.

(1) Automated Intelligence Record System (Pathfinder), JUSTICE/DEA-INS-111.

These exemptions apply to the extent that information in those systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) The system of records listed under paragraph (a) of this section is exempted, for the reasons set forth from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3)(d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, or the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and
lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4)(e)(1). The notices of these systems of records published in the Federal Register set forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal or other law enforcement investigations, cases, and matters, the Immigration and Naturalization Service or the Drug Enforcement Administration will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(5)(e)(2). In a criminal investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6)(e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that these systems of records are exempted from subsections (f) and (d).

(8)(e)(4)(I). The categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.
(9)(e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal, civil, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsections (f)(2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(12)(g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(13)(h). Since an exemption is being claimed for subsection (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(14) In addition, exemption is claimed for these systems of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): subsections (e)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) to the extent that the records contained in
these systems are specifically authorized to be kept secret in the interests of national defense and foreign policy.

Official Citation:
[Order No. 742-77, 42 FR 40907, Aug. 12, 1977]

28 CFR Section 16.103: Exemption of the INTERPOL-United States National Central Bureau (INTERPOL-USNCB) System.

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2), and (3), (e)(4) (G) and (H), (e)(5) and (8), (f) and (g):

(1) The INTERPOL-United States National Central Bureau (INTERPOL-USNCB) (Department of Justice) INTERPOL-USNCB Records System (JUSTICE/INTERPOL-001).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of accounting disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement.

(2) From subsections (c)(4), (d), (e)(4) (G), and (H), (f) and (g) because these provisions concern individual access to records and such access might compromise ongoing investigations reveal investigatory techniques and confidential informants, and invade the privacy of private citizens who provide information in connection with a particular investigation.

(3) From subsection (e)(1) because information received in the course of an international criminal investigation may involve a violation of state or local law, and it is beneficial to maintain this information to provide investigative leads to state and local law enforcement agencies.

(4) From subsection (e)(2) because collecting information from the subject of criminal investigations would thwart the investigation by placing the subject on notice.
(5) From subsection (e)(3) because supplying an individual with a statement of the intended use of the requested information could compromise the existence of a confidential investigation, and may inhibit cooperation.

(6) From subsection (e)(5) because the vast majority of these records come from local criminal justice agencies and it is administratively impossible to ensure that the records comply with this provision. Submitting agencies are, however, urged on a continuing basis to ensure that their records are accurate and include all dispositions.

(7) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

Official Citation:
[Order No. 8-82, 47 FR 44255, Oct. 7, 1982, as amended by Order No. 6-86, 51 FR 15479, Apr. 24, 1986]


(a) The following system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k): CaseLink Document Database for Office of Special Counsel—Waco, JUSTICE/OSCW-001. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(b) Only that portion of this system which consists of criminal or civil investigatory information is exempted for the reasons set forth from the following subsections:

(1) Subsection (c)(3).

To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him or her would inform that individual of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties and civil remedies.
(2) Subsection (c)(4).

This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) Subsection (d)(1).

Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others.

(4) Subsection (d)(2).

Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(5) Subsections (d)(3) and (4).

These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) Subsections (e)(1) and (5).

It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete; but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide leads in criminal investigations.

(7) Subsection (e)(2).

To collect information from the subject individual would serve notice that he or she is the subject of criminal investigative or law enforcement activity and thereby present a serious impediment to law enforcement.

(8) Subsection (e)(3).

To inform individuals as required by this subsection would reveal the existence of an investigation and compromise law enforcement efforts.

(9) Subsection (e)(8).
To serve notice would give persons sufficient warning to evade law enforcement efforts.

(10) Subsection (g).

This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:


(a) The following system of records is exempt from 5 U.S.C. 552a, subsections (c)(3), (d)(1), (2), (3) and (4), and (e)(1) and (4)(I): Flight Training Candidates File System (JUSTICE/FITTF-001). This exemption applies only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

(b) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures could reveal information that is classified in the interest of national security.

(2) From subsection (d)(1), (2), (3) and (4) because access to and amendment of certain portions of records within the system would tend to reveal or compromise information classified in the interest of national security.

(3) From subsection (e)(1) because it is often impossible to determine in advance if information obtained will be relevant for the purposes of conducting the risk analysis for flight training candidates.

(4) From subsection (e)(4)(I) to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than have been published in the Federal Register. Should the subsection be so interpreted, exemption from this provision is necessary because greater specificity concerning the sources of these records could compromise national security.

Official Citation:
(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d)(1), (2), (3) and (4), (e)(1), (2), and (3), (e)(4)(G), (H) and (I), (e)(5) and (8), (f) and (g).


2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(b) Exemptions from the particular subsections are justified for the following reasons:

1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest not only of ATF, but also of the recipient agency. This would permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.

2) From subsection (c)(4) because an exemption being claimed for subsection (d) makes this subsection inapplicable.

3) From subsections (d)(1), (e)(4)(G) and (H), (f) and (g) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information, including actual or potential tax information, which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

4) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to
continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because: (i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) In any investigation, ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

(7) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(8) From subsection (e)(3) because disclosure would provide the subject with substantial information that could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take steps to evade the investigation or flee a specific area.

(9) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such
exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(10) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(c) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Internal Security Record System (JUSTICE/ATF-006).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2) and (k)(5). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement investigation, and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or other measures.

(2) From subsection (d)(1) because disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Such breaches would restrict the free flow of information which is vital to the law enforcement process and the determination of an applicant's qualifications.
(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because it is often impossible to determine in advance if investigative records contained in this system are accurate, relevant, timely, complete, or of some assistance to either effective law enforcement investigations, or to the determination of the qualifications and suitability of an applicant. It also is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads. Information that may appear irrelevant, when combined with other apparently irrelevant information, can on occasion provide a composite picture of a subject or an applicant which assists the law enforcement process and the determination of an applicant's suitability qualifications.

(6) From subsection (e)(4)(G) and (H), and (f) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information, interfere with the overall law enforcement or qualification process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel. In addition, disclosure of information collected pursuant to an employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the objectivity or fairness of a testing or examination process.

(7) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.
(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Personnel Record System (JUSTICE/ATF-007).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(5). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal the existence, nature, or scope of an actual or potential personnel action. This would permit the record subject to take measures to hamper or impede such actions.

(2) From subsections (d)(1), (e)(4)(G) and (H), and (f) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a position with ATF. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of ATF. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate’s qualifications and suitability.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a personnel-related action.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.
(iii) ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

(6) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(g) The following systems of records are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Regulatory Enforcement Record System (JUSTICE/ATF-008).

(2) Technical and Scientific Services Record System (JUSTICE/ATF-009).

(3) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest, whether civil, criminal or regulatory, not only of ATF, but also of the recipient agency. This would permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation thus seriously hampering the regulatory and law enforcement functions of ATF.
(2) From subsections (d)(1), (e)(4)(G) and (H), and (f) because these provisions concern individual access to investigative and compliance records, disclosure of which could compromise sensitive information, interfere with the overall law enforcement and regulatory process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information, including actual or potential tax information, which would constitute an unwarranted invasion of another individual’s personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations and compliance actions attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal, civil, regulatory, or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative or regulatory activity can be established.

(iii) In any investigation or compliance action ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or compliance action or to an investigative activity under the jurisdiction of another agency.

(6) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the Federal Register in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act
requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal, regulatory, and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

**Official Citation:**

28 CFR Section 16.130:  Exemption of Department of Justice Systems: Correspondence Management Systems for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).

(a) The following Department of Justice systems of records are exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(1) Correspondence Management Systems (CMS) for the Department of Justice (DOJ), DOJ/003.

(2) Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ), DOJ/004.

(b) These systems are exempted for the reasons set forth from the following subsections:

(1) Subsection (c)(3).

To provide the subject of a criminal, civil, or counterintelligence matter or case under investigation with an accounting of disclosures of records concerning him or her could inform that individual of the existence, nature, or scope of that investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.
(2) Subsection (c)(4).

This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) Subsection (d)(1).

Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) Subsection (d)(2).

Amendment of the records would interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) Subsections (d)(3) and (4).

These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) Subsection (e)(1).

It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) Subsection (e)(2).

To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) Subsection (e)(3).

To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.
(9) Subsection (e)(5).

It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) Subsection (e)(8).

To serve notice could give persons sufficient warning to evade investigative efforts.

(11) Subsection (g).

This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:

28 CFR Section 16.131: Exemption of Department of Justice (DOJ)/Nationwide Joint Automated Booking System (JABS), DOJ-005.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2), (3), (4)(G) and (H), (e)(5) and (8), (f) and (g): Nationwide Joint Automated Booking System, Justice/DOJ-005. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Where compliance would not interfere with or adversely affect the law enforcement process, the DOJ may waive the exemptions, either partially or totally.

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3), (c)(4), and (d) to the extent that access to records in this system of records may impede or interfere with law enforcement efforts, result in the disclosure of information that would constitute an unwarranted invasion of the personal privacy of collateral record subjects or other third parties, and/or jeopardize the health and/or safety of third parties.
(2) From subsection (e)(1) to the extent that it is necessary to retain all information in order not to impede, compromise, or interfere with law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law enforcement agencies in discharging their law enforcement responsibilities.

(3) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement since it may be necessary to obtain and verify information from a variety to sources other than the record subject to ensure safekeeping, security, and effective law enforcement. For example, it maybe necessary that medical and psychiatric personnel provide information regarding the subject's behavior, physical, health, or mental stability, etc. to ensure proper care while in custody, or it may be necessary to obtain information from a case agent or the court to ensure proper disposition of the subject individual.

(4) From subsection (e)(3) because the requirement that agencies inform each individual whom it asks to supply information of such information as is required by subsection (e)(3) may, in some cases, impede the information gathering process or otherwise interfere with or compromise law enforcement efforts, e.g., the subject may deliberately withhold information, or give erroneous information.

(5) From subsection (4)(G) and(H) because the application of these provisions would present a serious impediment to law enforcement efforts.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes, may prevent the eventual development of the necessary criminal intelligence, or otherwise impede law enforcement or delay trained law enforcement personnel from timely exercising their judgment in managing the arrestee.

(7) From subsection (e)(8) to the extent that such notice may impede, interfere with, or otherwise compromise law enforcement and security efforts.

(8) From subsection 5 U.S.C. 552a(f) to the extent that compliance with the requirement for procedures providing individual access to records, compliance could impede, compromise, or interfere with law enforcement efforts.
(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

**Official Citation:**

28 CFR Section 16.132: Exemption of Department of Justice System—Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006.

(a) The following Department of Justice system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1),(2),(3),(5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k): Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(b) Exemption from the particular subsections is justified for the following reasons:

   (1) Subsection (e)(3).

   To provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

   (2) Subsection (e)(4).

   This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

   (3) Subsection (d)(1).

   Disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Disclosure of classified national security information would cause damage to the national security of the United States.
(4) Subsection (d)(2).

Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) Subsections (d)(3) and (4).

These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) Subsection (e)(1).

It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) Subsection (e)(2).

To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) Subsection (e)(3).

To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) Subsection (e)(5).

It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) Subsection (e)(8).

To serve notice could give persons sufficient warning to evade investigative efforts.
(11) Subsection (g).

This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

Official Citation:

28 CFR Section 16.133: Exemption of Department of Justice Regional Data Exchange System (RDEX), DOJ-012.

(a) The Department of Justice Regional Data Exchange System (RDEX), DOJ-012, is exempted from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) This system is exempted from the following subsections for the reasons set forth below:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures of criminal law enforcement records concerning him or her could inform that individual of the existence, nature, or scope of an investigation, or could otherwise seriously impede law enforcement efforts.

(2) From subsection (c)(4) because this system is exempt from subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of criminal law enforcement information could interfere with an investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others.

(4) From subsection (d)(2) because amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent that exemption is claimed from subsections (d)(1) and (2).
(6) From subsection (e)(1) because it is often impossible to determine in advance if criminal law enforcement records contained in this system are relevant and necessary, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) From subsection (e)(2) because collecting information from the subject individual could serve notice that he or she is the subject of a criminal law enforcement matter and thereby present a serious impediment to law enforcement efforts. Further, because of the nature of criminal law enforcement matters, vital information about an individual frequently can be obtained only from other persons who are familiar with the individual and his or her activities and it often is not practicable to rely on information provided directly by the individual.

(8) From subsection (e)(3) because informing individuals as required by this subsection could reveal the existence of a criminal law enforcement matter and compromise criminal law enforcement efforts.

(9) From subsection (e)(5) because it is often impossible to determine in advance if criminal law enforcement records contained in this system are accurate, relevant, timely, and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and obtaining investigative leads.

(10) From subsection (e)(8) because serving notice could give persons sufficient warning to evade criminal law enforcement efforts.

(11) From subsection (g) to the extent that this system is exempt from other specific subsections of the Privacy Act.

**Official Citation:**
[Order No. 007-2005, 70 FR 49870, Aug. 25, 2005]
SUBPART F—Public Observation of Parole Commission Meetings

Source:
42 FR 14713, Mar. 16, 1977, unless otherwise noted.


As used in this part:

(a) The term Commission means the U.S. Parole Commission and any subdivision thereof authorized to act on its behalf.

(b) The term meeting refers to the deliberations of at least the number of Commissioners required to take action on behalf of the Commission where such deliberations determine or result in the joint conduct or disposition of official Commission business.

(c) Specifically included in the term meeting are;

(1) Meetings of the Commission required to be held by 18 U.S.C. 4203(a);

(2) Special meetings of the Commission called pursuant to 18 U.S.C. 4204(a)(1);

(3) Meetings of the National Commissioners in original jurisdiction cases pursuant to 28 CFR 2.17(a);

(4) Meetings of the entire Commission to determine original jurisdiction appeal cases pursuant to 28 CFR 2.27; and

(5) Meetings of the National Appeals Board pursuant to 28 CFR 2.26.

(6) Meetings of the Commission to conduct a hearing on the record in conjunction with applications for certificates of exemption under section 504(a) of the Labor-Management Reporting and Disclosure Act of 1959, and section 411

(d) Specifically excluded from the term meeting are:

   (1) Determination made through independent voting of the Commissioners without the joint deliberation of the number of Commissioners required to take such action, pursuant to § 16.201;

   (2) Original jurisdiction cases determined by sequential vote pursuant to 28 CFR 2.17;

   (3) Cases determined by sequential vote pursuant to 28 CFR 2.24 and 2.25;

   (4) National Appeals Board cases determined by sequential vote pursuant to 28 CFR 2.26;

   (5) Meetings of special committees of Commissioners not constituting a quorum of the Commission, which may be established by the Chairman to report and make recommendations to the Commission or the Chairman on any matter.

   (6) Determinations required or permitted by these regulations to open or close a meeting, or to withhold or disclose documents or information pertaining to a meeting.

(e) All other terms used in this part shall be deemed to have the same meaning as identical terms used in chapter I, part 2 of this title.

Official Citation:

Part 4a was removed at 44 FR 6890, Feb. 2, 1979.
28 CFR Section 16.201: Voting by the Commissioners without joint deliberation.

(a) Whenever the Commission's Chairman so directs, any matter which (1) does not appear to require joint deliberation among the members of the Commission, or (2) by reason of its urgency, cannot be scheduled for consideration at a Commission meeting, may be disposed of by presentation of the matter separately to each of the members of the Commission. After consideration of the matter each Commission member shall report his vote to the Chairman.

(b) Whenever any member of the Commission so requests, any matter presented to the Commissioners for disposition pursuant to paragraph (a) of this section shall be withdrawn and scheduled instead for consideration at a Commission meeting.

(c) The provisions of § 16.206(a) of these rules shall apply in the case of any Commission determination made pursuant to this section.


(a) Every portion of every meeting of the Commission shall be open to public observation unless closed to the public pursuant to the provisions of § 16.203 (Formal Procedure) or § 16.205 (Informal Procedure).

(b) The attendance of any member of the public is conditioned upon the orderly demeanor of such person during the conduct of Commission business. The public shall be permitted to observe and to take notes, but unless prior permission is granted by the Commission, shall not be permitted to record or photograph by means of any mechanical or electronic device any portion of meetings which are open to the public.

(c) The Commission shall be responsible for arranging a suitable site for each open Commission meeting so that ample seating, visibility, and acoustics are provided to the public and ample security measures are employed for the protection of Commissioners and Staff. The Commission shall be responsible for recording or developing the minutes of Commission meetings.

(d) Public notice of open meetings shall be given as prescribed in § 16.204(a), and a record of votes kept pursuant to § 16.206(a).

28 CFR Section 16.203: Closed meetings—Formal procedure.
(a) The Commission, by majority vote, may close to public observation any meeting or portion thereof, and withhold from the public announcement concerning such meeting any information, if public observation or the furnishing of such information is likely to:

(1) Disclose matters:

   (i) Specifically authorized under criteria established by an executive order to be kept secret in the interests of national defense or foreign policy and

   (ii) In fact properly classified pursuant to such executive order;

(2) Relate solely to the internal personnel rules and practices of the Commission or any agency of the Government of the United States;

(3) Disclose matters specifically exempted from disclosure by statute (other than 5 U.S.C. 552, or the Federal Rules of Criminal Procedure): Provided, that such statute or rule (i) requires that the matters be withheld in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld, including exempted material under the Privacy Act of 1974 or the Commission's Alternate Means of Access under the Privacy Act of 1974, as set forth at 28 CFR 16.85;

(4) Disclose a trade secret or commercial or financial information obtained from any person, corporation, business, labor or pension organization, which is privileged or obtained upon a promise of confidentiality, including information concerning the financial condition or funding of labor or pension organizations, or the financial condition of any individual, in conjunction with applications for exemption under 29 U.S.C. 504 and 1111, and information concerning income, assets and liabilities of inmates, and persons on supervision;

(5) Involve accusing any person of a crime or formally censuring any person;

(6) Disclose information of a personal nature, where disclosure would constitute a clearly unwarranted invasion of personal privacy;

(7) Disclose an investigatory record compiled for law enforcement purposes, or information derived from such a record, which describes the criminal history or associations of any person under the Commission's jurisdiction or which describes the involvement of any person in the commission of a crime, but only to the extent that the production of such records or information would:
(i) Interfere with enforcement proceedings;

(ii) Deprive a person of a right to a fair trial or an impartial adjudication;

(iii) Constitute an unwarranted invasion of personal privacy;

(iv) Disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source;

(v) Disclose investigative techniques and procedures, or

(vi) Endanger the life or physical safety of law enforcement personnel;

(8) Disclose information, the premature disclosure of which would be likely to significantly frustrate implementation of proposed Commission action except where

(i) The Commission has already publicly disclosed the content or nature of its proposed action or

(ii) The Commission is required by law to make such disclosure on its own initiative prior to taking final Commission action on such proposal;

(9) Specifically concern the Commission’s issuance of subpoena or participation in a civil action or proceeding; or

(10) Specifically concern the initiation, conduct, or disposition of a particular case of formal adjudication pursuant to the procedures in 5 U.S.C. 554, or of any case involving a determination on the record after opportunity for a hearing. Included under the above terms are:
(i) Record review hearings following opportunity for an in-person hearing pursuant to the procedures of 28 CFR 4.1 through 4.17 and 28 CFR 4a.1 through 4a.17\(^5\) (governing applications for certificates of exemption under the Labor-Management Reporting and Disclosure Act of 1959 and the Employee Retirement Income Security Act of 1974), and

(ii) The initiation, conduct, or disposition by the Commission of any matter pursuant to the procedures of 28 CFR 2.1 through 2.58 (parole, release, supervision, and recommitment of prisoners, youth offenders, and juvenile delinquents).

(b) Public interest provision.
Notwithstanding the exemptions at paragraphs (a)(1) through (a)(10) of this section, the Commission may conduct a meeting or portion of a meeting in public when the Commission determines, in its discretion, that the public interest in an open meeting clearly outweighs the need for confidentiality.

(c) Nonpublic matter in announcements.
The Commission may delete from any announcement or notice required in these regulations information the disclosure of which would be likely to have any of the consequences described in paragraphs (a)(1) through (a)(10) of this section, including the name of any individual considered by the Commission in any case of formal or informal adjudication.

(d) Voting and certification.
(1) A separate recorded vote of the Commission shall be taken with respect to each meeting or portion thereof which is proposed to be closed, and with respect to any information which is proposed to be withheld pursuant to this section. Voting by proxy shall not be permitted. In the alternative, the Commission may, by a single majority vote, close to public observation a series of meetings, or portion(s) thereof or withhold information concerning such series of meetings, provided that:

(i) Each meeting in such series involves the same particular matters, and

\(^5\) Part 4a was removed at 44 FR 6890, Feb. 2, 1979.
(ii) Each meeting is scheduled to be held no more than thirty days after the initial meeting in the series.

(2) Upon the request of any Commissioner, the Commission shall make a determination as to closure pursuant to this subsection if any person whose interests may be directly affected by a portion of a meeting requests the Commission to close such portion or portions to the public observation for any of the grounds specified in paragraph (a) (5), (6) or (7) of this section.

(3) The determination to close any meeting to public observation pursuant to this section shall be made at least one week prior to the meeting or the first of a series of meetings as the case may be. If a majority of the Commissioners determines by recorded vote that agency business requires the meeting to take place at any earlier date, the closure determination and announcement thereof shall be made at the earliest practicable time. Within one day of any vote taken on whether to close a meeting under this section, the Commission shall make available to the public a written record reflecting the vote of each Commissioner on the question, including a full written explanation of its action in closing the meeting, portion(s) thereof, or series of meetings, together with a list of all persons expected to attend the meeting(s) or portion(s) thereof and their affiliation, subject to the provisions of paragraph (c) of this section.

(4) For every meeting or series of meetings closed pursuant to this section, the General Counsel of the Parole Commission shall publicly certify that, in Counsel’s opinion, the meeting may be closed to the public and shall state each relevant exemptive provision.

28 CFR Section 16.204: Public notice.

(a) Requirements.
Every open meeting and meeting closed pursuant to § 16.203 shall be preceded by a public announcement posted before the main entrance to the Chairman’s Office at the Commission's headquarters, 5550 Friendship Boulevard, Chevy Chase, Maryland 20815-7286, and, in the case of a meeting held elsewhere, in a prominent place at the location in which the meeting will be held. Such announcement shall be transmitted to the Federal Register for publication and, in addition, may be issued through the Department of Justice, Office of Public Affairs, as a press release, or by such other means as the Commission shall deem reasonable and appropriate. The announcement shall furnish:

(1) A brief description of the subject matter to be discussed;

(2) The date, place, and approximate time of the meeting;
(3) Whether the meeting will be open or closed to public observation; and

(4) The name and telephone number of the official designated to respond to requests for information concerning the meeting. See § 16.205(d) for the notice requirement applicable to meetings closed pursuant to that section.

(b) Time of notice.
The announcement required by this section shall be released to the public at least one week prior to the meeting announced therein except where a majority of the members of the Commission determines by a recorded vote that Commission business requires earlier consideration. In the event of such a determination, the announcement shall be made at the earliest practicable time.

(c) Amendments to notice.
The time or place of a meeting may be changed following the announcement only if the Commission publicly announces such change at the earliest practicable time. The subject matter of a meeting, or determination of the Commission to open or close a meeting, or portion of a meeting, to the public may be changed following the announcement only if:

(1) A majority of the entire membership of the Commission determines by a recorded vote that Commission business so requires and that no earlier announcement of the change was possible, and

(2) The Commission publicly announces such change and the vote of each member upon such change at the earliest practicable time: Provided, that individual items which have been announced for Commission consideration at a closed meeting may be deleted without notice.

Official Citation:
public pursuant to 5 U.S.C. 552 (d)(4) and (c)(10). The major part of normal Commission business lies in the adjudication of individual parole cases, all of which proceedings commence with an initial parole or revocation hearing and are determined on the record thereof.

Original jurisdiction cases are decided at bi-monthly meetings of the National Commissioners (28 CFR 2.17) and by the entire Commission in conjunction with each business meeting of the Commission (held at least quarterly) (28 CFR 2.27).

The National Appeals Board normally decides cases by sequential vote on a daily basis, but may meet from time to time for joint deliberations. In the period from October, 1975 through September, 1976, the National Appeals Board made 2,072 Appellate decisions.

Finally, over the last two years the Commission determined eleven cases under the Labor and Pension Acts, which are proceedings pursuant to 5 U.S.C. 554. The only meetings of the Commission not of an adjudicative nature involving the most sensitive inquiry into the personal background and behavior of the individual concerned, or involving sensitive financial information concerning the parties before the Commission, are the normal business meetings of the Commission, which are held at least quarterly.

(b) Meetings to which applicable. The following types of meetings may be closed in the event that a majority of the Commissioners present at the meeting, and authorized to act on behalf of the Commission, votes by recorded vote at the beginning of each meeting or portion thereof, to close the meeting or portions thereof:

(1) Original jurisdiction initial and appellate case deliberations conducted pursuant to 28 CFR 2.17 and 2.27;

(2) National Appeals Board deliberations pursuant to 28 CFR 2.26;

(3) Meetings of the Commission to conduct a hearing on the record regarding applications for certificates of exemption pursuant to the Labor-Management Reporting and Disclosure Act of 1959, 29 U.S.C. 504, and the

(c) Written record of action to close meeting. In the case of a meeting or portion of a meeting closed pursuant to this section, the Commission shall make available to the public as soon as practicable:

(1) A written record reflecting the vote of each member of the Commission to close the meeting; and

(2) A certification by the Commission's General Counsel to the effect that in Counsel's opinion, the meeting may be closed to the public, which certification shall state each relevant exemptive provision.

(d) Public notice. In the case of meetings closed pursuant to this section the Commission shall make a public announcement of the subject matter to be considered, and the date, place, and time of the meeting. The announcement described herein shall be released to the public at the earliest practicable time.

28 CFR Section 16.206: Transcripts, minutes, and miscellaneous documents concerning Commission meetings.

(a) In the case of any Commission meeting, whether open or closed, the Commission shall maintain and make available for public inspection a record of the final vote of each member on rules, statements of policy, and interpretations adopted by it: 18 U.S.C. 4203(d).

(b) The Commission shall maintain a complete transcript or electronic recording adequate to record fully the proceedings of each meeting, or portion of a meeting, closed to the public pursuant to § 16.203. In the case of a meeting, or portion of a meeting, closed to the public pursuant to § 16.205 of these regulations, the Commission may maintain either the transcript or recording described above, or

6 Part 4a was removed at 44 FR 6890, Feb. 2, 1979.
a set of minutes unless a recording is required by title 18 U.S.C. 4208(f). The minutes required by this section shall fully and clearly describe all matters discussed and shall provide a full and accurate summary of any actions taken, and the reasons therefor, including a description of each of the views expressed on any item and the record of any rollcall vote (reflecting the vote of each Commissioner on the question). All documents considered in connection with any action shall be identified in such minutes.

(c) The Commission shall retain a copy of every certification executed by the General Counsel's Office pursuant to these regulations, together with a statement from the presiding officer of the meeting, or portion of a meeting to which the certification applies, setting forth the time and place of the meeting, and the persons present.

(d) Nothing herein shall affect any other provision in Commission procedures or regulations requiring the preparation and maintenance of a record of all official actions of the Commission.

28 CFR Section 16.207: Public access to nonexempt transcripts and minutes of closed Commission meetings—Documents used at meetings—Record retention.

(a) Public access to records.
Within a reasonable time after any closed meeting, the Commission shall make available to the public, in the Commission's Public Reading Room located at 5550 Friendship Boulevard, Chevy Chase, Maryland 20815-7286, the transcript, electronic recording, or minutes of the discussion of any item on the agenda, or of any item of the testimony of any witness received at such meeting, maintained hereunder, except for such item or items of such discussion or testimony which contain information exempt under any provision of the Government in the Sunshine Act (Pub. L. 94-409), or of any amendment thereto. Copies of nonexempt transcripts, or minutes, or a transcription of such recording disclosing the identity of each speaker, shall be furnished to any person at the actual cost of duplication or transcription.

(b) Access to documents identified or discussed in any Commission meeting, open or closed, shall be governed by Department of Justice regulations at this part 16, subparts C and D.
The Commission reserves the right to invoke statutory exemptions to disclosure of such documents under 5 U.S.C. 552 and 552a, and applicable regulations. The exemptions provided in 5 U.S.C. 552b(c) shall apply to any request made pursuant to 5 U.S.C. 552 or 552a to copy and inspect any transcripts, recordings or minutes prepared or maintained pursuant hereto.
(c) Retention of records.
The Commission shall maintain a complete verbatim copy of the transcript, or a complete copy of the minutes, or a complete electronic recording of each meeting, or portion of a meeting, closed to the public, for a period of at least two years after such meeting, or until one year after the conclusion of any Commission proceeding with respect to which the meeting or portion thereof was held, whichever occurs later.

**Official Citation:**

**28 CFR Section 16.208: Annual report.**

The Commission shall report annually to Congress regarding its compliance with Sunshine Act requirements, including a tabulation of the total number of meetings open to the public, the total number of meetings closed to the public, the reasons for closing such meetings, and a description of any litigation brought against the Commission under this section, including any costs assessed against the Commission in such litigation and whether or not paid.
SUBPART G—Access to Documents by Former Employees of the Department

Source:
Order No. 2333-2000, 65 FR 68892, Nov. 15, 2000, unless otherwise noted.


(a) To the extent permitted by law, former employees of the Department shall be given access to documents that they originated, reviewed, or signed while employees of the Department, for the purpose of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority. Documents include memoranda, drafts, reports, notes, written communications, and documents stored electronically that are in the possession of the Department. Access ordinarily will be provided on government premises.

(b) Requests for access to documents under this section must be submitted in writing to the head of the component where the employee worked when originating, reviewing, or signing the documents. If the employee requesting access was the Attorney General, Deputy Attorney General, or Associate Attorney General, the request may be granted by the Assistant Attorney General for Administration. This authority may not be delegated below the level of principal deputy component head.

(c) The written request should describe with specificity the documents to which access is sought (including time periods wherever possible), the reason for which access is sought (including the timing of the official inquiry involved), and any intended disclosure of any of the information contained in the documents.

(d) The requester must agree in writing to safeguard the information from unauthorized disclosure and not to further disclose the information, by any means of communication, or to make copies, without the permission of the Department. Determinations regarding any further disclosure of information or removal of copies shall be made in accordance with applicable standards and procedures.

28 CFR Section 16.301: Limitations.

(a) The Department may deny or limit access under this subpart where providing the requested access would be unduly burdensome.
(b) Access under this subpart to classified information is governed by Executive Order 12958 and 28 CFR 17.46. Requests for access to classified information must be submitted to (or will be referred to) the Department Security Officer and may be granted by the Department Security Officer in consultation with the appropriate component head.

(c) Nothing in this subpart shall be construed to supplant the operation of other applicable prohibitions against disclosure.

(d) This subpart is not intended to, does not, and may not be relied upon to, create any right or benefit, substantive or procedural, enforceable at law by a party against the United States.
APPENDIX I TO PART 16—COMPONENTS OF THE DEPARTMENT OF JUSTICE

Unless a separate address is listed below, the address for each component is: [component name], U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001. For all components marked by an asterisk, FOIA and Privacy Act requests should be sent to the Office of Information and Privacy, U.S. Department of Justice, Flag Bldg., Suite 570, Washington, DC 20530-0001. The components are:

A
Office of the Attorney General *
Office of the Deputy Attorney General *
Office of the Associate Attorney General *
Office of the Solicitor General

B
Office of Information and Privacy *
Office of the Inspector General
Office of the Intelligence Policy and Review
Office of Intergovernmental Affairs *
Office of Investigative Agency Policies
Office of Legal Counsel
Office of Legislative Affairs *
Office of Policy Development *
Office of Professional Responsibility
Office of Public Affairs *

C
Antitrust Division, U.S. Department of Justice, LPB Bldg., Suite 200, Washington, DC 20530-0001
Civil Division, U.S. Department of Justice, 901E Bldg., Room 808, Washington, DC 20530-0001

Civil Rights Division, U.S. Department of Justice, NYAV Bldg., Room 8000B, Washington, DC 20530-0001

Criminal Division, U.S. Department of Justice, WCTR Bldg., Suite 1075, Washington, DC 20530-0001

Environment and Natural Resources Division, U.S. Department of Justice, Post Office Box 4390, Washington, DC 20044-4390

Justice Management Division

Tax Division, U.S. Department of Justice, JCB Bldg., Room 6823, Washington, DC 20530-0001

Bureau of Alcohol, Tobacco, Firearms, and Explosives, U.S. Department of Justice, Washington, DC 20226

Bureau of Prisons, U.S. Department of Justice, HOLC Bldg., Room 738, 320 First Street, NW., Washington, DC 20534-0001


Drug Enforcement Administration, U.S. Department of Justice, Washington, DC 20537-0001

Executive Office for Immigration Review, U.S. Department of Justice, Suite 2400, 5107 Leesburg Pike, Falls Church, VA 22041-0001

Executive Office for United States Attorneys, U.S. Department of Justice, BICN Bldg., Room 7100, Washington, DC 20530-0001

Executive Office for United States Trustees, U.S. Department of Justice, 901E Bldg., Room 780, Washington, DC 20530-0001

Federal Bureau of Investigation, U.S. Department of Justice, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001 (for field offices, consult your telephone book)

Foreign Claims Settlement Commission, U.S. Department of Justice, BICN Bldg., Room 6002, 600 E Street, NW., Washington, DC 20579-0001
Immigration and Naturalization Service, U.S. Department of Justice, CAB Bldg., 425 Eye Street, NW., Washington, DC 20536-0001 (for field offices, consult your telephone book)

INTERPOL-U.S. National Central Bureau, U.S. Department of Justice, Washington, DC 20530-0001

National Drug Intelligence Center, U.S. Department of Justice, Fifth Floor, 319 Washington Street, Johnstown, PA 15901-1622

Office of Community Oriented Policing Services, U.S. Department of Justice, VT1 Bldg., Twelfth Floor, Washington, DC 20530-0001

Office of Justice Programs, U.S. Department of Justice, Room 5337, 810 Seventh Street, NW., Washington, DC 20531-0001

Pardon Attorney, U.S. Department of Justice, FRST Bldg., Fourth Floor, Washington, DC 20530-0001

United States Marshals Service, U.S. Department of Justice, Lincoln Place, Room 1250, CSQ3, 600 Army Navy Drive, Arlington, VA 22202-4210

**Official Citation:**
28 CFR PART 17—CLASSIFIED NATIONAL SECURITY INFORMATION AND ACCESS TO CLASSIFIED INFORMATION

- 28 CFR Section 17.1: Purpose.
- 28 CFR Section 17.2: Scope.
- 28 CFR Section 17.3: Definitions.

Subpart A—Administration
- 28 CFR Section 17.11: Authority of the Assistant Attorney General for Administration.
- 28 CFR Section 17.12: Component head responsibilities.
- 28 CFR Section 17.14: Department Review Committee.
- 28 CFR Section 17.15: Access Review Committee.
- 28 CFR Section 17.16: Violations of classified information requirements.
- 28 CFR Section 17.17: Judicial proceedings.
- 28 CFR Section 17.18: Prepublication review.

Subpart B—Classified Information
- 28 CFR Section 17.21: Classification and declassification authority.
- 28 CFR Section 17.22: Classification of information; limitations.
- 28 CFR Section 17.23: Emergency classification requests.
- 28 CFR Section 17.24: Duration of classification.
- 28 CFR Section 17.25: Identification and markings.
- 28 CFR Section 17.26: Derivative classification.
- 28 CFR Section 17.27: Declassification and downgrading.
- 28 CFR Section 17.28: Automatic declassification.
- 28 CFR Section 17.29: Documents of permanent historical value.
- 28 CFR Section 17.30: Classification challenges.
- 28 CFR Section 17.31: Mandatory review for declassification requests.
- 28 CFR Section 17.32: Notification of classification changes.

Subpart C—Access to Classified Information
- 28 CFR Section 17.41: Access to classified information.
- 28 CFR Section 17.42: Positions requiring financial disclosure.
- 28 CFR Section 17.43: Reinvestigation requirements.
- 28 CFR Section 17.44: Access eligibility.
- 28 CFR Section 17.45: Need-to-know.
- 28 CFR Section 17.46: Access by persons outside the Executive Branch.
- 28 CFR Section 17.47: Denial or revocation of eligibility for access to classified information.

Authority:

Source:
Order No. 2091-97, 62 FR 36984, July 10, 1997, unless otherwise noted.
The purpose of this part is to ensure that information within the Department of Justice (the “Department”) relating to the national security is classified, protected, and declassified pursuant to the provisions of Executive Orders 12958 (3 CFR, 1995 Comp., p. 333) and 12968 (3 CFR, 1995 Comp., p. 391) and implementing directives from the Information Security Oversight Office of the National Archives and Records Administration (“ISOO”). Executive Orders 12958 and 12968 made numerous substantive changes in the system of classification, declassification, and downgrading of classified National Security Information and the criteria for access to this information. Accordingly, this part is a revision of the Department’s classified information security rules.

(a) Subpart A of this part prescribes the implementation of Executive Orders 12958 and 12968 within the Department through the Assistant Attorney General for Administration, as the senior responsible agency official. Subpart A of this part also provides for certain relationships within the Department between the Assistant Attorney General for Administration, other component heads, and the National Security Division.

(b) Subpart B of this part prescribes an orderly and progressive system for ensuring that every necessary safeguard and procedure is in place to assure that information is properly classified and that classified information is protected from unauthorized disclosure. Subpart B of this part requires original classification authorities to make classification decisions based on specific criteria; provides that most newly created classified information be considered for declassification after 10 years; provides that historically valuable information that is more than 25 years old (including information classified under prior Executive Orders) be automatically declassified, with appropriate exceptions; and establishes procedures for authorized holders of classified information to challenge the classification of information.

(c) Subpart C of this part establishes substantive standards and procedures for granting, denying, and revoking, and for appealing decisions to deny access to classified information with an emphasis on ensuring the consistent, cost-effective, and efficient protection of classified information. Subpart C of this part provides a process that is fair and equitable to those with whom classified information is entrusted and, at the same time, assures the security of the classified information.

Official Citation:
28 CFR Section 17.2: Scope.

(a) All employees, contractors, grantees, and others granted access to classified information by the Department are governed by this part, and by the standards in Executive Order 12958, Executive Order 12968, and directives promulgated under those Executive Orders. If any portion of this part conflicts with any portion of Executive Order 12958, Executive Order 12968, or any successor Executive Order, the Executive Order shall apply. This part supersedes the former rule and any Department internal operating policy or directive that conflicts with any portion of this part.

(b) This part applies to non-contractor personnel outside of the Executive Branch and to contractor personnel or employees who are entrusted with classified national security information originated within or in the custody of the Department. This part does not affect the operation of the Department’s participation in the National Industrial Security Program under Executive Order 12829 (3 CFR, 1993 Comp., p. 570).

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person. This part creates limited rights to administrative review of decisions pursuant to §§ 17.30, 17.31, and 17.47. This part does not, and is not intended to, create any right to judicial review of administrative action under §§ 17.14, 17.15, 17.18, 17.27, 17.30, 17.31 and 17.50.

28 CFR Section 17.3: Definitions.

The terms defined or used in Executive Order 12958 and Executive Order 12968, and the implementing directives in 32 CFR 2001, are applicable to this part.
(a) The Assistant Attorney General for Administration is designated as the senior agency official as required by § 5.6(c) of Executive Order 12958, and § 6.1(a) of Executive Order 12968 and, except as specifically provided elsewhere in this part, is authorized to administer the Department's national security information program pursuant to Executive Order 12958. The Assistant Attorney General for Administration shall appoint a Department Security Officer and may delegate to the Department Security Officer those functions under Executive Orders 12958 and 12968 that may be delegated by the senior agency official. The Department Security Officer may redelegated such functions when necessary to effectively implement this part.

(b) The Assistant Attorney General for Administration shall, among other actions:

(1) Oversee and administer the Department’s program established under Executive Order No. 12958;

(2) Establish and maintain Department-wide security education and training programs;

(3) Establish and maintain an ongoing self-inspection program including the periodic review and assessment of the Department's classified product;

(4) Establish procedures to prevent unnecessary access to classified information, including procedures that:

   (i) Require that a need for access to classified information is established before initiating administrative procedures to grant access; and

   (ii) Ensure that the number of persons granted access to classified information is limited to the minimum necessary for operational and security requirements and needs;

(5) Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(6) Assure that the performance contract or other system used to rate personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

   (i) Original classification authorities;
(ii) Security managers or security specialists; and

(iii) All other personnel whose duties significantly involve the creation or handling of classified information;

(7) Account for the costs associated with implementing this part and report the cost to the Director of the ISOO;

(8) Assign in a prompt manner personnel to respond to any request, appeal, challenge, complaint, or suggestion concerning Executive Order 12958 that pertains to classified information that originated in a component of the Department that no longer exists and for which there is no clear successor in function;

(9) Cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines;

(10) Conduct periodic evaluations of the Department's implementation and administration of Executive Orders 12958 and 12968;

(11) Establish a plan for compliance with the automatic declassification provisions of Executive Order 12958 and oversee the implementation of that plan; and

(12) Maintain a list of specific files series of records exempted from automatic declassification by the Attorney General pursuant to section 3.4(c) of Executive Order 12958.

(c) The Department Security Officer may grant, deny, suspend, or revoke employee access to classified information pursuant to and in accordance with Executive Order 12968. The Department Security Officer may delegate the authority under this paragraph to qualified Security Programs Managers when the operational need justifies the delegation and when the Department Security Officer is assured that such officials will apply all access criteria in a uniform and correct manner in accord with the provisions of Executive Order 12968 and subpart C of this part. The fact that a delegation has been made pursuant to this section does not waive the Department Security Officer's authority to make any determinations that have been delegated.

(d) The Department Security Officer shall maintain a current list of all officials authorized pursuant to this part to originally classify or declassify documents.
(e) The Department Security Officer shall promulgate criteria and security requirements for the marking and safeguarding of information, transportation and transfer of information, preparation of classification guides, reporting of communications related to national security by persons granted access to classified information, reporting of information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security, and other matters necessary to the administration of the Executive Orders, the implementing regulations of the ISOO, and this part.

28 CFR Section 17.12: Component head responsibilities.

The head of each component shall appoint and oversee a Security Programs Manager to implement this regulation. The Security Programs Managers shall:

(a) Observe, enforce, and implement security regulations or procedures pertaining to the classification, declassification, safeguarding, handling, and storage of classified national security information;

(b) Report violations of the provisions of this regulation to the Department Security Officer;

(c) Ensure that all employees acquire adequate security education and training as required by the provisions of the Department security regulations and procedures for classified information;

(d) Continuously review the requirements for personnel access to classified information as a part of the continuous need-to-know evaluation, and initiate action to administratively withdraw or reduce the level of access authorized, as appropriate; and

(e) Cooperate fully with any request from the Department Security Officer for assistance in the implementation of this part.


(a) The Assistant Attorney General for National Security or a designee shall represent the Attorney General at interagency meetings on matters of general interest concerning national security information.
(b) The Assistant Attorney General for National Security shall provide advice and interpretation on any issues that arise under Executive Orders 12958 and 12968 and shall refer such questions to the Office of Legal Counsel, as appropriate.

(c) Any request for interpretation of Executive Order 12958 or Executive Order 12968, pursuant to section 6.1(b) of Executive Order 12958, and section 7.2(b) of Executive Order 12968, shall be referred to the Assistant Attorney General for National Security, who shall refer such questions to the Office of Legal Counsel, as appropriate.

**Official Citation:**

---

28 CFR Section 17.14: Department Review Committee.

(a) The Department Review Committee (DRC) is established to:

(1) Resolve all issues, except those related to the compromise of classified information, that concern the implementation and administration of Executive Order 12958, implementing directives from the ISOO, and subpart B of this part, including those issues concerning over-classification, failure to declassify, classification challenges, and delays in declassification not otherwise resolved;

(2) Review all appeals from denials of requests for records made under section 3.6 of Executive Order 12958 and the Freedom of Information Act (5 U.S.C. 552), when the proposed denial is based on their continued classification under Executive Order 12958;

(3) Recommend to the Attorney General appropriate administrative sanctions to correct the abuse or violation of any provision of Executive Order 12958, the implementing directives or subpart B of this part, except as it relates to the compromise of classified national security information; and

(4) Review, on appeal, challenges to classification actions and mandatory review requests.

(b)(1) The DRC shall consist of a senior representative designated by the:

(i) Deputy Attorney General;

(ii) Assistant Attorney General, Office of Legal Counsel;

(iii) Assistant Attorney General, Criminal Division;
(iv) Assistant Attorney General, Civil Division;

(v) Assistant Attorney General for National Security;

(vi) Assistant Attorney General for Administration; and

(vii) Director, Federal Bureau of Investigation.

(2) Each such official shall also designate in writing an alternate to serve in the absence of his or her representative. Four representatives shall constitute a quorum of the DRC. The Attorney General shall designate the Chairman of the DRC from among its members.

(c) The Office of Information and Privacy (OIP) shall provide the necessary administrative staff support for the DRC.

Official Citation:

28 CFR Section 17.15: Access Review Committee.

(a) The Access Review Committee (ARC) is hereby established to review all appeals from denials or revocations of eligibility for access to classified information under Executive Order 12968. Unless the Attorney General requests recommendations from the ARC and personally exercises appeal authority, the ARC’s decisions shall be final.

(b) The ARC shall consist of the Deputy Attorney General or a designee, the Assistant Attorney General for National Security or a designee, and the Assistant Attorney General for Administration or a designee. Designations must be approved by the Attorney General.

(c) The Department Security Officer shall provide the necessary administrative staff support for the ARC.

Official Citation:
28 CFR Section 17.16: Violations of classified information requirements.

(a) Any person who suspects or has knowledge of a violation of this part, including the known or suspected loss or compromise of national security information, shall promptly report and confirm in writing the circumstances to the Department Security Officer. Any person who makes such a report to the Department Security Officer shall promptly furnish a copy of such report:

(1) If the suspected violation involves a Department attorney (including an Assistant United States Attorney or Special Assistant United States Attorney) while engaged in litigation, grand jury proceedings, or giving legal advice, or a law enforcement officer assisting an attorney engaged in such activity, to the Office of Professional Responsibility;

(2) If the suspected violation involves an employee of the Federal Bureau of Investigation (FBI) or the Drug Enforcement Administration, other than a law enforcement officer in paragraph (a)(1) of this section, to the Office of Professional Responsibility in that component; or

(3) In any other circumstance, to the Office of the Inspector General.

(b) Department employees, contractors, grantees, or consultants may be reprimanded, suspended without pay, terminated from classification authority, suspended from or denied access to classified information, or subject to other sanctions in accordance with applicable law and Department regulation if they:

(1) Knowingly, willfully, or negligently disclose to unauthorized persons information classified under Executive Order 12958 or predecessor orders;

(2) Knowingly, willfully, or negligently classify or continue the classification of information in violation of Executive Order 12958 or its implementing directives; or

(3) Knowingly, willfully, or negligently violate any other provision of Executive Order 12958, or knowingly and willfully grant eligibility for, or allow access to, classified information in violation of Executive Order 12968, or its implementing directives, this part, or security requirements promulgated by the Department Security Officer.

28 CFR Section 17.17: Judicial proceedings.
(a)(1) Any Department official or organization receiving an order or subpoena from a federal or state court to produce classified information, required to submit classified information for official Department litigative purposes, or receiving classified information from another organization for production of such in litigation, shall immediately determine from the agency originating the classified information whether the information can be declassified. If declassification is not possible, the Department official or organization and the assigned Department attorney in the case shall take all appropriate action to protect such information pursuant to the provisions of this section.

(2) If a determination is made to produce classified information in a judicial proceeding in any manner, the assigned Department attorney shall take all steps necessary to ensure the cooperation of the court and, where appropriate, opposing counsel in safeguarding and retrieving the information pursuant to the provisions of this regulation.


(c) In judicial proceedings other than Federal criminal cases where CIPA is used, the Department, through its attorneys, shall seek appropriate security safeguards to protect classified information from unauthorized disclosure, including, but not limited to, consideration of the following:

(1) A determination by the court of the relevance and materiality of the classified information in question;

(2) An order that classified information shall not be disclosed or introduced into evidence at a proceeding without the prior approval of either the originating agency, the Attorney General, or the President;

(3) A limitation on attendance at any proceeding where classified information is to be disclosed to those persons with appropriate authorization to access classified information whose duties require knowledge or possession of the classified information to be disclosed;

(4) A court facility that provides appropriate safeguarding for the classified information as determined by the Department Security Officer;

(5) Dissemination and accountability controls for all classified information offered for identification or introduced into evidence at such proceedings;
(6) Appropriate marking to indicate classified portions of any and any the maintenance of any classified under seal;

(7) Handling and storage of all classified information including classified portions of any transcript in a manner consistent with the provisions of this regulation and Department implementing directives;

(8) Return at the conclusion of the proceeding of all classified information to the Department or the originating agency, or placing the classified information under court seal;

(9) Retrieval by Department employees of appropriate notes, drafts, or any other documents generated during the course of the proceedings that contain classified information and immediate transfer to the Department for safeguarding and destruction as appropriate; and

(10) Full and complete advice to all persons to whom classified information is disclosed during such proceedings as to the classification level of such information, all pertinent safeguarding and storage requirements, and their liability in the event of unauthorized disclosure.

(d) Access to classified information by individuals involved in judicial proceedings other than employees of the Department is governed by § 17.46(c).

28 CFR Section 17.18: Prepublication review.

(a) All individuals with authorized access to Sensitive Compartmented Information shall be required to sign nondisclosure agreements containing a provision for prepublication review to assure deletion of Sensitive Compartmented Information and other classified information. Sensitive Compartmented Information is information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods. The prepublication review provision will require Department of Justice employees and other individuals who are authorized to have access to Sensitive Compartmented Information to submit certain material, described further in the agreement, to the Department prior to its publication to provide an opportunity for determining whether an unauthorized disclosure of Sensitive Compartmented Information or other classified information would occur as a consequence of its publication.
(b) Persons subject to these requirements are invited to discuss their plans for public disclosures of information that may be subject to these obligations with authorized Department representatives at an early stage, or as soon as circumstances indicate these policies must be considered. Except as provided in paragraph (j) of this section for FBI personnel, all questions concerning these obligations should be addressed to the Assistant Attorney General for National Security, Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530. The official views of the Department on whether specific materials require prepublication review may be expressed only by the Assistant Attorney General for National Security and persons should not act in reliance upon the views of other Department personnel.

(c) Prepublication review is required only as expressly provided for in a nondisclosure agreement. However, all persons who have had access to classified information have an obligation to avoid unauthorized disclosures of such information. Therefore, persons who have such access but are not otherwise required to submit to prepublication review under the terms of an employment or other nondisclosure agreement are encouraged to submit material for prepublication review voluntarily if they believe that such material may contain classified information.

(d) The nature and extent of the material that is required to be submitted for prepublication review under nondisclosure agreements is expressly provided for in those agreements. It should be clear, however, that such requirements do not extend to any materials that exclusively contain information lawfully obtained at a time when the author has no employment, contract, or other relationship with the United States Government or that contain information exclusively acquired outside the scope of employment.

(e) A person’s obligation to submit material for prepublication review remains identical whether such person prepares the materials or causes or assists another person (such as a ghost writer, spouse, friend, or editor) in preparing the material. Material covered by a nondisclosure agreement requiring prepublication review must be submitted prior to discussing it with or showing it to a publisher, co-author, or any other person who is not authorized to have access to it. In this regard, it should be noted that a failure to submit such material for prepublication review constitutes a breach of the obligation and exposes the author to remedial action even in cases where the published material does not actually contain Sensitive Compartmented Information or classified information. See Snepp v. United States, 444 U.S. 507 (1980).

(f) The requirement to submit material for prepublication review is not limited to any particular type of material or disclosure or methods of production. Written materials include not only book manuscripts but all other forms of written materials intended for public disclosure, such as (but not limited to) newspaper
columns, magazine articles, letters to the editor, book reviews, pamphlets, scholarly papers, and fictional material.

(g) Oral statements are also within the scope of a prepublication review requirement when based upon written materials, such as an outline of the statements to be made. There is no requirement to prepare written materials for review, however, unless there is reason to believe in advance that oral statements may contain Sensitive Compartmented Information or other information required to be submitted for review under the terms of the nondisclosure agreement. Thus, a person may participate in an oral presentation where there is no opportunity for prior preparation (e.g., news interview, panel discussion) without violating the provisions of this paragraph.

(h) Material submitted for republication review will be reviewed solely for the purpose of identifying and preventing the disclosure of Sensitive Compartmented Information and other classified information. This review will be conducted in an impartial manner without regard to whether the material is critical of or favorable to the Department. No effort will be made to delete embarrassing or critical statements that are unclassified. Materials submitted for review will be disseminated to other persons or agencies only to the extent necessary to identify classified information.

(i) The Assistant Attorney General for National Security or a designee (or, in the case of FBI employees, the Section Chief, Records/Information Dissemination Section, Records Management Division) will respond substantively to prepublication review requests within 30 working days of receipt of the submission. Priority shall be given to reviewing speeches, newspaper articles, and other materials that the author seeks to publish on an expedited basis. The Assistant Attorney General’s decisions may be appealed to the Deputy Attorney General, who will process appeals within 15 days of receipt of the appeal. The Deputy Attorney General’s decision is final and not subject to further administrative appeal. Persons who are dissatisfied with the final administrative decision may obtain judicial review either by filing an action for declaratory relief, or by giving the Department notice of their intention to proceed with publication despite the Department’s request for deletions of classified information and giving the Department 30 working days to file a civil action seeking a court order prohibiting disclosure. Employees and other affected individuals remain obligated not to disclose or publish information determined by the Government to be classified until any civil action is resolved.

(j) The obligations of Department of Justice employees described in this subpart apply with equal force to employees of the FBI with following exceptions and provisos:

(1) Nothing in this subpart shall supersede or alter obligations assumed under the basic FBI employment agreement.
(2) FBI employees required to sign nondisclosure agreements containing a provision for prepublication review pursuant to this subpart shall submit materials for review to the Section Chief, Records/Information Dissemination Section, Records Management Division. Such individuals shall also submit questions as to whether specific materials require prepublication review under such agreements to that Section for resolution. Where such questions raise policy questions or concern significant issues of interpretation under such an agreement, the Section Chief, Records/Information Dissemination Section, Records Management Division, shall consult with the Assistant Attorney General for National Security, or a designee, prior to responding to the inquiry.

(3) Decisions of the Section Chief, Records/Information Dissemination Section, Records Management Division, concerning the deletion of classified information, may be appealed to the Director, FBI, who will process appeals within 15 working days of receipt. Persons who are dissatisfied with the Director’s decision may, at their option, appeal further to the Deputy Attorney General as provided in paragraph (i) of this section. Judicial review, as set forth in that paragraph, is available following final agency action in the form of a decision by the Director, if the appeal process in paragraph (i) of this section is pursued, the Deputy Attorney General.

Official Citation:
SUBPART B—Classified Information

28 CFR Section 17.21: Classification and declassification authority.

(a) Top Secret original classification authority may only be exercised by the Attorney General, the Assistant Attorney General for Administration, and officials to whom such authority is delegated in writing by the Attorney General. No official who is delegated Top Secret classification authority pursuant to this paragraph may redelegate such authority.

(b) The Assistant Attorney General for Administration may delegate original Secret and Confidential classification authority to subordinate officials determined to have frequent need to exercise such authority. No official who is delegated original classification authority pursuant to this paragraph may redelegate such authority.

(c) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level. In the absence of an official authorized to exercise classification authority pursuant to this section, the person designated to act in lieu of such official may exercise the official’s classification authority.

28 CFR Section 17.22: Classification of information; limitations.

(a) Information may be originally classified only if all of the following standards are met:

(1) The information is owned by, produced by or for, or is under the control of the United States Government;

(2) The information falls within one or more of the categories of information specified in section 1.5 of Executive Order 12958; and

(3) The classifying official determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and such official is able to identify or describe the damage.

(b) Information may be classified as Top Secret, Secret, or Confidential according to the standards established in section 1.3 of Executive Order 12958. No other terms shall be used to identify United States classified national security information except as otherwise provided by statute.

(c) Information shall not be classified if there is significant doubt about the need to classify the information. If there is significant doubt about the appropriate
level of classification with respect to information that is being classified, it shall be classified at the lower classification of the levels considered.

(d) Information shall not be classified in order to conceal inefficiency, violations of law, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay release of information that does not require protection in the interest of national security. Information that has been declassified and released to the public under proper authority may not be reclassified.

(e) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after the Department has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of § 17.31. When it is necessary to classify or reclassify such information, it shall be forwarded to the Department Security Officer and classified or reclassified only at the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for Administration.

(f) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that meets the standards for classification under Executive Order 12958 and that is not otherwise revealed in the individual items of information.

28 CFR Section 17.23: Emergency classification requests.

(a) Whenever any employee, contractor, licensee, certificate holder, or grantee of the Department who does not have original classification authority originates or develops information that requires immediate classification and safeguarding, and no authorized classifier is available, that person shall:

   (1) Safeguard the information in a manner appropriate for its classification level;

   (2) Apply the appropriate overall classification markings; and

   (3) Within five working days, securely transmit the information to the organization that has appropriate subject matter interest and classification authority.

(b) When it is not clear which Department organization would be the appropriate original classifier, the information shall be sent to the Department Security Officer to determine the appropriate organization.
(c) The organization with classification authority shall decide within 30 days whether to classify information.

28 CFR Section 17.24: Duration of classification.

(a) At the time of original classification, original classification authorities shall attempt to establish a specific date or event for declassification not more than 10 years from the date of the original decision based on the duration of the national security sensitivity of the information. If the original classification authority cannot determine an earlier specific date or event for declassification, the information shall be marked for declassification 10 years from the date of the original decision.

(b) At the time of original classification, an original classification authority may exempt specific information from declassification within 10 years in accordance with section 1.6(d) of Executive Order 12958.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under, and subject to the limitations of, Executive Order 12958.

28 CFR Section 17.25: Identification and markings.

(a) Classified information must be marked pursuant to the standards set forth in section 1.7 of Executive Order 12958; ISOO implementing directives in 32 CFR 2001, subpart B; and internal Department of Justice direction provided by the Department Security Officer.

(b) Foreign government information shall be marked or classified at a level equivalent to that level of classification assigned by the originating foreign government.

(c) Information assigned a level of classification under predecessor Executive Orders shall be considered as classified at that level of classification.

28 CFR Section 17.26: Derivative classification.
(a) Persons need not possess original classification authority to derivatively classify information based on source documents or classification guides.

(b) Persons who apply derivative classification markings shall observe original classification decisions and carry forward to any newly created documents the pertinent classification markings.

(c) Information classified derivatively from other classified information shall be classified and marked in accordance with the standards set forth in sections 2.1-2.3 of Executive Order 12958, the ISOO implementing directives in 32 CFR 2001.22, and internal Department directions provided by the Department Security Officer.

28 CFR Section 17.27: Declassification and downgrading.

(a) Classified information shall be declassified as soon as it no longer meets the standards for classification. Declassification and downgrading is governed by §3.1-3.3 of Executive Order 12958, implementing ISOO directives at 32 CFR 2001, subpart E, and applicable internal Department of Justice direction provided by the Department Security Officer.

(b) Information shall be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, the originator's successor, or a supervisory official of either, or by officials delegated such authority in writing by the Attorney General or the Assistant Attorney General for Administration.

(c) It is presumed that information that continues to meet the classification requirements under Executive Order 12958 requires continued protection. In some exceptional cases during declassification reviews, the need to protect classified information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. If it appears that the public interest in disclosure of the information may outweigh the need to protect the information, the declassification reviewing official shall refer the case with a recommendation for decision to the DRC. The DRC shall review the case and make a recommendation to the Attorney General on whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. The Attorney General shall decide whether to declassify the information. The decision of the Attorney General shall be final. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review.
(d) Each component shall develop schedules for declassification of records in the National Archives. The Department shall cooperate with the National Archives and Records Administration and the Presidential Libraries to ensure that declassification is accomplished in a timely manner.

28 CFR Section 17.28: Automatic declassification.

(a) Subject to paragraph (b) of this section, all classified information contained in records that are more than 25 years old that have been determined to have permanent historical value shall be declassified automatically on April 17, 2000. Subsequently, all classified information in such records shall be automatically declassified not later than 25 years after the date of its original classification with the exception of specific information exempt from automatic declassification pursuant to section 3.4 (b) and (d) of Executive Order 12958.

(b) At least 220 days before information is declassified automatically under this section, the respective component head shall notify the Assistant Attorney General for Administration through the Department Security Officer of any specific information they propose to exempt from automatic declassification. The notification shall include:

(1) A description of the information;

(2) An explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) A specific date or event for declassification of the information whenever the information exempted does not identify a confidential human source or human intelligence source.

(c) Proposed exemptions under this section shall be forwarded to the DRC, which shall recommend a disposition of the exemption request to the Assistant Attorney General for Administration. When the Assistant Attorney General for Administration determines the exemption request is consistent with this section, he or she will submit it to the Executive Secretary of the Interagency Security Classification Appeals Panel.

(d) Declassification guides that narrowly and precisely define exempted information may be used to exempt information from automatic declassification. Declassification guides must include the exemption notification information detailed in paragraph (b) of this section, and be approved pursuant to paragraph (c) of this section.
28 CFR Section 17.29: Documents of permanent historical value.

The original classification authority, to the greatest extent possible, shall declassify classified information contained in records determined to have permanent historical value under title 44 of the United States Code before they are accessioned into the National Archives. The Department shall cooperate with the National Archives and Records Administration in carrying out an automatic declassification program involving accessioned Department records, presidential papers, and historical materials under the control of the Archivist of the United States.

28 CFR Section 17.30: Classification challenges.

(a) Authorized holders of information classified by the Department who, in good faith, believe that specific information is improperly classified or unclassified are encouraged and expected to challenge the classification status of that information pursuant to section 1.9 of Executive Order 12958. Authorized holders may submit classification challenges in writing to the DRC, through the Office of Information and Privacy, United States Department of Justice, Washington, DC 20530. The challenge need not be more specific than a question as to why the information is or is not classified, or is classified at a certain level.

(b) The DRC shall redact the identity of an individual challenging a classification under paragraph (a) of this section and forward the classification challenge to the original classification authority for review and response.

(c) The original classification authority shall promptly, and in no case later than 30 days, provide a written response to the DRC. The original classification authority may classify or declassify the information subject to challenge or state specific reasons why the original classification determination was proper. If the original classification authority is not able to respond within 30 days, the DRC shall inform the individual who filed the challenge in writing of that fact, and the anticipated determination date.

(d) The DRC shall inform the individual challenging the classification of the determination made by the original classification authority and that individual may appeal this determination to the DRC. Upon appeal, the DRC may declassify, or direct the classification of, the information. If the DRC is not able to act on any appeal within 45 days of receipt, the DRC shall inform the individual who filed the challenge in writing of that fact, and the anticipated determination date.

(e) The DRC shall provide the individual who appeals a classification challenge determination with a written explanation of the basis for the DRC decision and a
statement of his or her right to appeal that determination to the Interagency Security Classification Appeals Panel (ISCAP) pursuant to section 5.4 of Executive Order 12958 and the rules issued by the ISCAP pursuant to section 5.4 of Executive Order 12958.

(f) Any individual who challenges a classification and believes that any action has been taken against him or her in retribution because of that challenge shall report the facts to the Office of the Inspector General or the Office of Professional Responsibility, as appropriate.

(g) Requests for review of classified material for declassification by persons other than authorized holders are governed by § 17.31.

28 CFR Section 17.31: Mandatory review for declassification requests.

(a) Any person may request classified information be reviewed for declassification pursuant to the mandatory declassification review provisions of section 3.6 of Executive Order 12958. After such a review, the information or any reasonably segregable portion thereof that no longer requires protection under this part shall be declassified and released to the requester unless withholding is otherwise warranted under applicable law. If the information, although declassified, is withheld, the requester shall be given a brief statement as to the reasons for denial and a notice of the right to appeal the determination to the Director, Office of Information and Privacy (OIP), United States Department of Justice, Washington, DC 20530. If the mandatory review for declassification request relates to the classification of information that has been reviewed for declassification within the past two years or that is the subject of pending litigation, the requester shall be informed of that fact and the administrative appeal rights.

(b) Request for mandatory review for declassification and any subsequent appeal to the DRC shall be submitted to the Director, Office of Information and Privacy, United States Department of Justice, Washington, DC 20530, describing the document or material containing the information with sufficient specificity to enable the Department to locate that information with a reasonable amount of effort. The OIP shall promptly forward the request to the component that originally classified the information, or the DRC in the case of an appeal, and provide the requester with an acknowledgement of receipt of the request.

(c) When the description of the information in a request is deficient, the component shall solicit as much additional identifying information as possible from the requestor. Before denying a request on the basis that the information or
material is not obtainable with a reasonable amount of effort, the component shall ask the requestor to limit the request to information or material that is reasonably obtainable. If the information or material requested cannot be described in sufficient particularity, or if it cannot be obtained with a reasonable amount of effort, the component shall provide the requestor with written notification of the reasons why no action will be taken and the right to appeal the decision to the DRC.

(d) The component that originally classified the information shall provide a written response to requests for mandatory review within 60 days whenever possible, or shall inform the requester in writing why additional time is needed. Unless there are unusual circumstances, the additional time needed by the component originally classifying the information shall not extend beyond 180 days from the receipt of the request. If no determination has been made at the end of the 180 day period, the requester may apply to the DRC for a determination.

(e) If the component that originally classified the information determines that continued classification is warranted, it shall notify the requester in writing of the decision and the right to appeal the decision to the DRC no later than 60 days after receipt of the notification of the decision.

(f) The DRC shall determine the appeals of the components’ mandatory declassification review decisions within 60 days after receipt of the appeal, or notify the requester why additional time is needed. In making its determinations concerning requests for declassification of classified information, the DRC, for administrative purposes, shall impose the burden of proof on the originating component to show that continued classification is warranted. The DRC shall provide the requester with a written statement of reasons for its decisions.

(g) If the individual requesting review of a classification is not satisfied with the DRC’s decision, he or she may appeal to the ISCAP pursuant to section 5.4 of Executive Order 12958 and rules issued by the ISCAP pursuant to that section.

28 CFR Section 17.32: Notification of classification changes.

All known holders of information affected by unscheduled classification changes actions shall be notified promptly of such changes by the original classifier or the authority making the change in classification.
(a) No person may be given access to classified information or material originated by, in the custody, or under the control of the Department, unless the person—

   (1) Has been determined to be eligible for access in accordance with sections 3.1-3.3 of Executive Order 12968;

   (2) Has a demonstrated need-to-know; and

   (3) Has signed an approved nondisclosure agreement.

(b) Eligibility for access to classified information is limited to United States citizens for whom an appropriate investigation of their personal and professional history affirmatively indicated loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of the national security. Sections 2.6 and 3.3 of Executive Order 12968 provide only limited exceptions to these requirements.

(c) The Department of Justice does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information. However, the Department may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No negative inferences concerning the standards for access may be raised solely on the basis of the sexual orientation of the employee or mental health counseling.

(d) An employee granted access to classified information may be investigated at any time to ascertain whether he or she continues to meet the requirements for access.

(e) An employee granted access to classified information shall provide to the Department written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of three years thereafter, to:
(1) Financial records maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in 12 U.S.C. 3401;

(2) Consumer reports under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); and

(3) Records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(f) Information may be requested pursuant to the employee consent obtained under paragraph (e) of this section only where:

(1) There are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(2) Information the Department deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or

(3) Circumstances indicate that the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

28 CFR Section 17.42: Positions requiring financial disclosure.

(a) The Assistant Attorney General for Administration, in consultation with the Assistant Attorney General for National Security, shall designate each employee, by position or category where possible, who has a regular need for access to any of the categories of classified information described in section 1.3(a) of Executive Order 12968.

(b) An employee may not hold a position designated as requiring a regular need for access to categories of classified information described in section 1.3(a) of Executive Order 12968 unless, as a condition of access to such information, the employee files with the Department Security Officer:

(1) A financial disclosure form developed pursuant to section 1.3(c) of Executive Order 12968 as part of all background investigations or reinvestigations;
(2) The same financial disclosure form, if selected by the Department Security Officer on a random basis; and

(3) Relevant information concerning foreign travel, as determined by the Department Security Officer.

**Official Citation:**

**28 CFR Section 17.43: Reinvestigation requirements.**

Employees who are eligible for access to classified information shall be subject to periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access.

**28 CFR Section 17.44: Access eligibility.**

(a) Determinations of eligibility for access to classified information are separate from suitability determinations with respect to the hiring or retention of persons for employment by the Department or any other personnel actions.

(b) The number of employees eligible for access to classified information shall be kept to the minimum required for the conduct of Department functions.

(c) Eligibility for access to classified information shall be limited to classification levels for which there is a need for access. No person shall be granted eligibility higher than his or her need.

**28 CFR Section 17.45: Need-to-know.**

No person shall be granted access to specific classified information unless that person has an actual need-to-know that classified information, pursuant to section 2.5 of Executive Order 12968.

**28 CFR Section 17.46: Access by persons outside the Executive Branch.**
(a) Classified information shall not be disseminated outside the Executive Branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the Executive Branch.

(b) Classified information originated by or in the custody of the Department may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Federal Government will derive a benefit or advantage and that the release is not prohibited by the originating department or agency (or foreign government in the case of Foreign Government Information). Before such a release is made, the head of the Office, Board, Division, or Bureau making the release shall determine the propriety of such action, in the interest of the national security, and must approve the release. Prior to the release, the Department Security Officer must confirm that the recipient is eligible for access to the classified information involved and agrees to safeguard the information in accordance with the provisions of this part.

(c) Members of Congress, Justices of the United States Supreme Court, and Judges of the United States Courts of Appeal and District Courts do not require a determination of their eligibility for access to classified information by the Department. Federal Magistrate Judges must be determined eligible for access to classified information by the Department Security Officer pursuant to procedures approved by the Assistant Attorney General for Administration in consultation with the Judicial Conference of the United States. All other Legislative and Judicial personnel including, but not limited to, congressional staff, court reporters, typists, secretaries, law clerks, and translators who require access to classified information must be determined eligible by the Department Security Officer consistent with standards established in this regulation.

(d) When other persons outside the Executive Branch who are not subject to the National Industrial Security Program require access to classified information originated by or in the custody of the Department, but do not otherwise possess a proper access authorization, an appropriate background investigation must be completed to allow the Department Security Officer to determine their eligibility for access to classified information. The length of time it generally takes to complete an expedited background investigation is 90 days. Therefore, all persons requiring access to classified information to participate in congressional or judicial proceedings should be identified and the background investigation initiated far enough in advance to ensure a minimum impact on such proceedings.

(e) Personnel who are subject to a Department contract or grant or who are rendering consultant services to the Department and require access to classified information originated by or in the custody of the Department shall be processed
for such access pursuant to procedures approved by the Assistant Attorney General for Administration.

(f)(1) The requirement that access to classified information may be granted only as is necessary for the performance of official duties may be waived, pursuant to section 4.5(a) of Executive Order 12958, for persons who:

(i) Are engaged in historical research projects; or

(ii) Have previously occupied policymaking positions to which they were appointed by the President.

(2) All persons receiving access pursuant to this paragraph (f) must have been determined to be trustworthy by the Department Security Officer as a precondition before receiving access. Such determinations shall be based on such investigation as the Department Security Officer deems appropriate. Historical researchers and former presidential appointees shall not have access to Foreign Government Information without the written permission from an appropriate authority of the foreign government concerned.

(3) Waivers of the “need-to-know” requirement under this paragraph (f) may be granted by the Department Security Officer provided that the Security Programs Manager of the Office, Board, Division, or Bureau with classification jurisdiction over the information being sought:

(i) Makes a written determination that such access is consistent with the interest of national security;

(ii) Limits such access to specific categories of information over which the Department has classification jurisdiction;

(iii) Maintains custody of the classified information at a Department facility;

(iv) Obtains the recipient's written and signed agreement to safeguard the information in accordance with the provisions of this regulation and to authorize a review of any notes and manuscript for determination that no classified information is contained therein; and

(v) In the case of former presidential appointees, limits their access to items that such former appointees originated, reviewed, signed, or received while serving as a presidential appointee and ensures that such appointee does not remove or cause to be removed any classified information reviewed.

(4) If access requested by historical researchers and former presidential appointees requires the rendering of services for which fair and equitable fees
may be charged pursuant to 31 U.S.C. 9701, the requester shall be so notified and fees may be imposed.

28 CFR Section 17.47: Denial or revocation of eligibility for access to classified information.

(a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of Executive order 12968 shall be:

   (1) Provided with a comprehensive and detailed written explanation of the basis for that decision as the national security interests of the United States and other applicable law permit and informed of their right to be represented by counsel or other representative at their own expense;

   (2) Permitted 30 days from the date of the written explanation to request any documents, records, or reports including the entire investigative file upon which a denial or revocation is based; and

   (3) Provided copies of documents requested pursuant to this paragraph (a) within 30 days of the request to the extent such documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), and as the national security interests and other applicable law permit.

(b) An applicant or employee may file a written reply and request for review of the determination within 30 days after written notification of the determination or receipt of the copies of the documents requested pursuant to this subpart, whichever is later.

(c) An applicant or employee shall be provided with a written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal.

(d) Within 30 days of receipt of a determination under paragraph (c) of this section, the applicant or employee may appeal that determination in writing to the ARC, established under § 17.15. The applicant or employee may request an opportunity to appear personally before the ARC and to present relevant documents, materials, and information.

(e) An applicant or employee may be represented in any such appeal by an attorney or other representative of his or her choice, at his or her expense. Nothing in this section shall be construed as requiring the Department to grant
such attorney or other representative eligibility for access to classified information, or to disclose to such attorney or representative, or permit the applicant or employee to disclose to such attorney or representative, classified information.

(f) A determination of eligibility for access to classified information by the ARC is a discretionary security decision. Decisions of the ARC shall be in writing and shall be made as expeditiously as possible. Access shall be granted only where facts and circumstances indicate that access to classified information is clearly consistent with the national security interest of the United States, and any doubt shall be resolved in favor of the national security.

(g) The Department Security Officer shall have an opportunity to present relevant information in writing or, if the applicant or employee appears personally, in person. Any such written submissions shall be made part of the applicant’s or employee’s security record and, as the national security interests of the United States and other applicable law permit, shall also be provided to the applicant or employee. Any personal presentations shall be, to the extent consistent with the national security and other applicable law, in the presence of the applicant or employee.

(h) When the Attorney General or Deputy Attorney General personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This is a discretionary and final decision not subject to further review.

(i) This section does not limit the authority of the Attorney General pursuant to any other law or Executive Order to deny or terminate access to classified information if the national security so requires and the Attorney General determines that the appeal procedures set forth in this section cannot be invoked in a manner that is consistent with the national security. Nothing in this section requires that the Department provide any procedures under this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any reason other than denial of eligibility for access to classified information. Suitability determinations shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.
Subpart A—General Provisions
  - 28 CFR Section 20.1: Purpose.
  - 28 CFR Section 20.2: Authority.
  - 28 CFR Section 20.3: Definitions.

Subpart B—State and Local Criminal History Record Information Systems
  - 28 CFR Section 20.20: Applicability.
  - 28 CFR Section 20.21: Preparation and submission of a Criminal History Record Information Plan.
  - 28 CFR Section 20.23: Documentation: Approval by OJARS.

Subpart C—Federal Systems and Exchange of Criminal History Record Information
  - 28 CFR Section 20.30: Applicability.
  - 28 CFR Section 20.31: Responsibilities.
  - 28 CFR Section 20.32: Includable offenses.
  - 28 CFR Section 20.33: Dissemination of criminal history record information.
  - 28 CFR Section 20.34: Individual's right to access criminal history record information.
  - 28 CFR Section 20.35: Criminal Justice Information Services Advisory Policy Board.
  - 28 CFR Section 20.36: Participation in the Interstate Identification Index System.
  - 28 CFR Section 20.38: Sanction for noncompliance.
  - Appendix to Part 20—Commentary on Selected Sections of the Regulations on Criminal History Record Information Systems

Authority:

Source:
Order No. 601-75, 40 FR 22114, May 20, 1975, unless otherwise noted.
SUBPART A—General Provisions

Source:
41 FR 11714, Mar. 19, 1976, unless otherwise noted.

28 CFR Section 20.1: Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

Official Citation:
[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

28 CFR Section 20.2: Authority.


28 CFR Section 20.3: Definitions.

As used in these regulations:


(b) Administration of criminal justice means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(c) Control Terminal Agency means a duly authorized state, foreign, or international criminal justice agency with direct access to the National Crime Information Center telecommunications
network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.

(d) Criminal history record information means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual’s involvement with the criminal justice system.

(e) Criminal history record information system means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of criminal history record information.

(f) Criminal history record repository means the state agency designated by the governor or other appropriate executive official or the legislature to perform centralized recordkeeping functions for criminal history records and services in the state.

(g) Criminal justice agency means:

(1) Courts; and

(2) A governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included.

(h) Direct access means having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of or intervention by any other party or agency.

(i) Disposition means information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to
mental incompetency, charge still pending due to insanity, charge still pending
due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo
contendere plea, convicted, youthful offender determination, deceased, deferred
disposition, dismissed-civil action, found insane, found mentally incompetent,
pardoned, probation before conviction, sentence commuted, adjudication
withheld, mistrial-defendant discharged, executive clemency, placed on
probation, paroled, or released from correctional supervision.

(j) Executive order
means an order of the President of the United States or the Chief Executive of a
state that has the force of law and that is published in a manner permitting
regular public access.

(k) Federal Service Coordinator
means a non-Control Terminal Agency that has a direct telecommunications line
to the National Crime Information Center network.

(l) Fingerprint Identification Records System or ―FIRS‖
means the following FBI records: Criminal fingerprints and/or related criminal
justice information submitted by authorized agencies having criminal justice
responsibilities; civil fingerprints submitted by federal agencies and civil
generations submitted by persons desiring to have their fingerprints placed on
record for personal identification purposes; identification records, sometimes
referred to as "rap sheets," which are compilations of criminal history record
information pertaining to individuals who have criminal fingerprints maintained
in the FIRS; and a name index pertaining to all individuals whose fingerprints are
maintained in the FIRS. See the FIRS Privacy Act System Notice periodically
published in the Federal Register for further details.

(m) Interstate Identification Index System or ―III System‖
means the cooperative federal-state system for the exchange of criminal history
records, and includes the National Identification Index, the National Fingerprint
File, and, to the extent of their participation in such system, the criminal history
record repositories of the states and the FBI.

(n) National Crime Information Center or ―NCIC‖
means the computerized information system, which includes telecommunications
lines and any message switching facilities that are authorized by law, regulation,
or policy approved by the Attorney General of the United States to link local,
state, tribal, federal, foreign, and international criminal justice agencies for the
purpose of exchanging NCIC related information. The NCIC includes, but is not
limited to, information in the III System. See the NCIC Privacy Act System Notice
periodically published in the Federal Register for further details.

(o) National Fingerprint File or ―NFF‖
means a database of fingerprints, or other uniquely personal identifying information, relating to an arrested or charged individual maintained by the FBI to provide positive identification of record subjects indexed in the III System.

(p) National Identification Index or “NII” means an index maintained by the FBI consisting of names, identifying numbers, and other descriptive information relating to record subjects about whom there are criminal history records in the III System.

(q) Nonconviction data means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; information discloseing that the police have elected not to refer a matter to a prosecutor, that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed; and information that there has been an acquittal or a dismissal.

(r) State means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(s) Statute means an Act of Congress or of a state legislature or a provision of the Constitution of the United States or of a state.

**Official Citation:**
[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

**SUBPART B—State and Local Criminal History Record Information Systems**

**Source:**
41 FR 11715, Mar. 19, 1976, unless otherwise noted.

**28 CFR Section 20.20: Applicability.**

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July

---

Page 515
1, 1973, pursuant to title I of the Act. Use of information obtained from the FBI Identification Division or the FBI/NCIC system shall also be subject to limitations contained in subpart C.

(b) The regulations in this subpart shall not apply to criminal history record information contained in:

(1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons;

(2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis;

(3) Court records of public judicial proceedings;

(4) Published court or administrative opinions or public judicial, administrative or legislative proceedings;

(5) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver’s, pilot’s or other operators’ licenses;

(6) Announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section. The regulations do not prohibit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship.

28 CFR Section 20.21: Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to OJARS by each State on March 16, 1976, to set forth all operational procedures, except those portions relating to dissemination and security. A supplemental plan covering these portions shall be submitted no later
than 90 days after promulgation of these amended regulations. The plan shall set forth operational procedures to—

(a) Completeness and accuracy.
Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information unless it can be assured that the most up-to-date disposition data is being used. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period.

(2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) Limitations on dissemination.
Insure that dissemination of nonconviction data has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision, or order, as construed by appropriate State or local officials or agencies;

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, insures the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;
(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section 524(a), and provide sanctions for the violation thereof. These dissemination limitations do not apply to conviction data.

(c) General policies on use and dissemination.

(1) Use of criminal history record information disseminated to noncriminal justice agencies shall be limited to the purpose for which it was given.

(2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.

(3) Subsection (b) does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order.

(d) Juvenile records.
Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need or supervision (or the equivalent) to noncriminal justice agencies is prohibited, unless a statute, court order, rule or court decision specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in paragraph (b) (3) and (4) of this section.

(e) Audit.
Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated. The reporting of a criminal justice transaction to a State, local or Federal repository is not a dissemination of information.

(f) Security.
Wherever criminal history record information is collected, stored, or disseminated, each State shall insure that the following requirements are satisfied by security standards established by State legislation, or in the absence
of such legislation, by regulations approved or issued by the Governor of the State.

(1) Where computerized data processing is employed, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information.

(2) Access to criminal history record information system facilities, systems operating environments, data file contents whether while in use or when stored in a media library, and system documentation is restricted to authorized organizations and personnel.

(3)(i) Computer operations, whether dedicated or shared, which support criminal justice information systems, operate in accordance with procedures developed or approved by the participating criminal justice agencies that assure that:

(a) Criminal history record information is stored by the computer in such manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

(b) Operation programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than criminal justice system terminals which are so designated.

(c) The destruction of records is limited to designated terminals under the direct control of the criminal justice agency responsible for creating or storing the criminal history record information.

(d) Operational programs are used to detect and store for the output of designated criminal justice agency employees all unauthorized attempts to penetrate any criminal history record information system, program or file.

(e) The programs specified in paragraphs (f)(3)(i) (b) and (d) of this section are known only to criminal justice agency employees responsible for criminal history record information system control or individuals and agencies pursuant to a specific agreement with the criminal justice agency to provide such programs and the program(s) are kept continuously under maximum security conditions.

(f) Procedures are instituted to assure that an individual or agency authorized direct access is responsible for (1) the physical security of criminal history record information under its control or in its custody and (2) the protection of such information from unauthorized access, disclosure or dissemination.
(g) Procedures are instituted to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(ii) A criminal justice agency shall have the right to audit, monitor and inspect procedures established above.

(4) The criminal justice agency will:

(i) Screen and have the right to reject for employment, based on good cause, all personnel to be authorized to have direct access to criminal history record information.

(ii) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

(iii) Institute procedures, where computer processing is not utilized, to assure that an individual or agency authorized direct access is responsible for

(a) The physical security of criminal history record information under its control or in its custody and

(b) The protection of such information from unauthorized access, disclosure, or dissemination.

(iv) Institute procedures, where computer processing is not utilized, to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(v) Provide that direct access to criminal history record information shall be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

(5) Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations.

(g) Access and review.
Insure the individual’s right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

---

Page 520
(1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual’s right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by § 20.3(b).

Official Citation:
[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61595, Dec. 6, 1977]


(a) Each State to which these regulations are applicable shall with the submission of its plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

(1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under § 20.21(g) must be completely operational;
(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and

(5) A listing setting forth categories of non-criminal justice dissemination. See § 20.21(b).

28 CFR Section 20.23: Documentation: Approval by OJARS.

Within 90 days of the receipt of the plan, OJARS shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by OJARS will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by March 1, 1978. A final certification shall be submitted on March 1, 1978.

Where a State finds it is unable to provide final certification that all required procedures as set forth in § 20.21 will be operational by March 1, 1978, a further extension of the deadline will be granted by OJARS upon a showing that the State has made a good faith effort to implement these regulations to the maximum extent feasible. Documentation justifying the request for the extension including a proposed timetable for full compliance must be submitted to OJARS by March 1, 1978. Where a State submits a request for an extension, the implementation date will be extended an additional 90 days while OJARS reviews the documentation for approval or disapproval. To be approved, such revised schedule must be consistent with the timetable and procedures set out below:

(a) July 31, 1978—Submission of certificate of compliance with:

(1) Individual access, challenge, and review requirements;

(2) Administrative security;

(3) Physical security to the maximum extent feasible.
(b) Thirty days after the end of a State's next legislative session—Submission to OJARS of a description of State policy on dissemination of criminal history record information.

(c) Six months after the end of a State's legislative session—Submission to OJARS of a brief and concise description of standards and operating procedures to be followed by all criminal justice agencies covered by OJARS regulations in complying with the State policy on dissemination.

(d) Eighteen months after the end of a State's legislative session—Submission to OJARS of a certificate attesting to the conduct of an audit of the State central repository and of a random number of other criminal justice agencies in compliance with OJARS regulations.

**Official Citation:**
[41 FR 11715, Mar. 19, 1976, as amended at 42 FR 61596, Dec. 6, 1977]

---

28 CFR Section 20.24: *State laws on privacy and security.*

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

28 CFR Section 20.25: *Penalties.*

Any agency or individual violating subpart B of these regulations shall be subject to a civil penalty not to exceed $10,000 for a violation occurring before September 29, 1999, and not to exceed $11,000 for a violation occurring on or after September 29, 1999. In addition, OJARS may initiate fund cut-off procedures against recipients of OJARS assistance.

**Official Citation:**
[41 FR 11715, Mar. 19, 1976, as amended by Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]
SUBPART C—Federal Systems and Exchange of Criminal History Record Information

Source:
Order No. 2258-99, 64 FR 52227, Sept. 28, 1999, unless otherwise noted.

28 CFR Section 20.30: Applicability.

The provisions of this subpart of the regulations apply to the III System and the FIRS, and to duly authorized local, state, tribal, federal, foreign, and international criminal justice agencies to the extent that they utilize the services of the III System or the FIRS. This subpart is applicable to both manual and automated criminal history records.

28 CFR Section 20.31: Responsibilities.

(a) The Federal Bureau of Investigation (FBI) shall manage the NCIC.

(b) The FBI shall manage the FIRS to support identification and criminal history record information functions for local, state, tribal, and federal criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by federal statute, state statute pursuant to Public Law 92-544, 86 Stat. 1115, Presidential executive order, or regulation or order of the Attorney General of the United States.

(c) The FBI CJIS Division may manage or utilize additional telecommunication facilities for the exchange of fingerprints, criminal history record related information, and other criminal justice information.

(d) The FBI CJIS Division shall maintain the master fingerprint files on all offenders included in the III System and the FIRS for the purposes of determining first offender status; to identify those offenders who are unknown in states where they become criminally active but are known in other states through prior criminal history records; and to provide identification assistance in disasters and for other humanitarian purposes.

(e) The FBI may routinely establish and collect fees for noncriminal justice fingerprint-based and other identification services as authorized by Federal law. These fees apply to Federal, State and any other authorized entities requesting fingerprint identification records and name checks for noncriminal justice purposes.
(1) The Director of the FBI shall review the amount of the fee periodically, but not less than every four years, to determine the current cost of processing fingerprint identification records and name checks for noncriminal justice purposes.

(2) Fee amounts and any revisions thereto shall be determined by current costs, using a method of analysis consistent with widely accepted accounting principles and practices, and calculated in accordance with the provisions of 31 U.S.C. 9701 and other Federal law as applicable.

(3) Fee amounts and any revisions thereto shall be published as a notice in the Federal Register.

(f) The FBI will collect a fee for providing noncriminal name-based background checks of the FBI Central Records System through the National Name Check Program pursuant to the authority in Pub. L. 101-515 and in accordance with paragraphs (e)(1), (2) and (3) of this section.

Official Citation:

28 CFR Section 20.32: Includable offenses.

(a) Criminal history record information maintained in the III System and the FIRS shall include serious and/or significant adult and juvenile offenses.

(b) The FIRS excludes arrests and court actions concerning nonserious offenses, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, and traffic violations (except data will be included on arrests for vehicular manslaughter, driving under the influence of drugs or liquor, and hit and run), when unaccompanied by a § 20.32(a) offense. These exclusions may not be applicable to criminal history records maintained in state criminal history record repositories, including those states participating in the NFF.

(c) The exclusions enumerated above shall not apply to federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of this subpart.
28 CFR Section 20.33: Dissemination of criminal history record information.

(a) Criminal history record information contained in the III System and the FIRS may be made available:

(1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies;

(2) To federal agencies authorized to receive it pursuant to federal statute or Executive order;

(3) For use in connection with licensing or employment, pursuant to Public Law 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law. Refer to § 50.12 of this chapter for dissemination guidelines relating to requests processed under this paragraph;

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses;

(5) To criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS);

(6) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/ information services for criminal justice agencies; and

(7) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director’s designee).

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the
receiving departments, related agencies, or service providers identified in paragraphs (a)(6) and (a)(7) of this section.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

(d) Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

28 CFR Section 20.34: Individual's right to access criminal history record information.

The procedures by which an individual may obtain a copy of his or her identification record from the FBI to review and request any change, correction, or update are set forth in §§ 16.30-16.34 of this chapter. The procedures by which an individual may obtain a copy of his or her identification record from a state or local criminal justice agency are set forth in § 20.34 of the appendix to this part.

28 CFR Section 20.35: Criminal Justice Information Services Advisory Policy Board.

(a) There is established a CJIS Advisory Policy Board, the purpose of which is to recommend to the FBI Director general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's CJIS Division.

(b) The Board includes representatives from state and local criminal justice agencies; members of the judicial, prosecutorial, and correctional segments of the criminal justice community; a representative of federal agencies participating in the CJIS systems; and representatives of criminal justice professional associations.

(c) All members of the Board will be appointed by the FBI Director.

(d) The Board functions solely as an advisory body in compliance with the provisions of the Federal Advisory Committee Act. Title 5, United States Code, Appendix 2.
28 CFR Section 20.36: Participation in the Interstate Identification Index System.

(a) In order to acquire and retain direct access to the III System, each Control Terminal Agency and Federal Service Coordinator shall execute a CJIS User Agreement (or its functional equivalent) with the Assistant Director in Charge of the CJIS Division, FBI, to abide by all present rules, policies, and procedures of the NCIC, as well as any rules, policies, and procedures hereinafter recommended by the CJIS Advisory Policy Board and adopted by the FBI Director.

(b) Entry or updating of criminal history record information in the III System will be accepted only from state or federal agencies authorized by the FBI. Terminal devices in other agencies will be limited to inquiries.


It shall be the responsibility of each criminal justice agency contributing data to the III System and the FIRS to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

28 CFR Section 20.38: Sanction for noncompliance.

Access to systems managed or maintained by the FBI is subject to cancellation in regard to any agency or entity that fails to comply with the provisions of subpart C of this part.
Appendix to Part 20—Commentary on Selected Sections of the Regulations on Criminal History Record Information Systems

Subpart A

§ 20.3(d).

The definition of criminal history record information is intended to include the basic offender-based transaction statistics/III System (OBTS/III) data elements. If notations of an arrest, disposition, or other formal criminal justice transaction occurs in records other than the traditional “rap sheet,” such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

The definition, however, does not extend to other information contained in criminal justice agency reports. Intelligence or investigative information (e.g., suspected criminal activity, associates, hangouts, financial information, and ownership of property and vehicles) is not included in the definition of criminal history information.

§ 20.3(g).

The definitions of criminal justice agency and administration of criminal justice in § 20.3(b) of this part must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies, as well as subunits of noncriminal justice agencies that perform the administration of criminal justice pursuant to a federal or state statute or executive order and allocate a substantial portion of their budgets to the administration of criminal justice. The above subunits of noncriminal justice agencies would include, for example, the Office of Investigation of the Food and Drug Administration, which has as its principal function the detection and apprehension of persons violating criminal provisions of the Federal Food, Drug and Cosmetic Act. Also included under the definition of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services, such as New York’s Division of Criminal Justice Services.

§ 20.3(i).

Disposition is a key concept in section 524(b) of the Act and in §§ 20.21(a)(1) and 20.21(b) of this part. It therefore is defined in some detail. The specific dispositions listed in this subsection are examples only and are not to be construed as excluding other, unspecified transactions concluding criminal proceedings within a particular agency.

§ 20.3(q).
The different kinds of acquittals and dismissals delineated in § 20.3(i) are all considered examples of nonconviction data.

Subpart B

§ 20.20(a).

These regulations apply to criminal justice agencies receiving funds under the Omnibus Crime Control and Safe Streets Act for manual or automated systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA’s authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicate manual files for purposes contrary to the letter and spirit of the regulations.

Regulation of manual systems, therefore, is authorized by section 524(b) when coupled with section 501 of the Act which authorizes the Administration to establish rules and regulations “necessary to the exercise of its functions * * *.”

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

Limitations as contained in subpart C also apply to information obtained from the FBI Identification Division or the FBI/NCIC System.

§ 20.20 (b) and (c).

Section 20.20 (b) and (c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know. Court records of public judicial proceedings are also exempt from the provisions of the regulations.

Section 20.20(b)(2) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person’s arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.
Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus, announcements of arrest, convictions, new developments in the course of an investigation may be made. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: “Was X arrested by your agency on January 3, 1975” and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal justice agency may respond to the inquiry. Conviction data as stated in § 20.21(b) may be disseminated without limitation.

§ 20.21.

The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor. The State has 90 days from the publication of these revised regulations to submit the portion of the plan covering §§ 20.21(b) and 20.21(f).

§ 20.21(a)(1).

Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to a statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately, through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.20(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word “should” is permissive; it suggests but does not mandate a central State repository.
The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user’s request within a reasonable time. Presently, comprehensive records of an individual’s transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-access needs of police and prosecutors. On the other hand, queries of the State central repository for most noncriminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

§ 20.21(b).

The limitations on dissemination in this subsection are essential to fulfill the mandate of section 524(b) of the Act which requires the Administration to assure that the “privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes.” The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

The regulations distinguish between conviction and nonconviction information insofar as dissemination is concerned. Conviction information is currently made available without limitation in many jurisdictions. Under these regulations, conviction data and pending charges could continue to be disseminated routinely. No statute, ordinance, executive order, or court rule is necessary in order to authorize dissemination of conviction data. However, nothing in the regulations shall be construed to negate a State law limiting such dissemination.

After December 31, 1977, dissemination of nonconviction data would be allowed, if authorized by a statute, ordinance, executive order, or court rule, decision, or order. The December 31, 1977, deadline allows the States time to review and determine the kinds of dissemination for non-criminal justice purposes to be authorized. When a State enacts comprehensive legislation in this area, such legislation will govern dissemination by local jurisdictions within the State. It is possible for a public record law which has been construed by the State to authorize access to the public of all State records, including criminal history record information, to be considered as statutory authority under this subsection. Federal legislation and executive orders can also authorize dissemination and would be relevant authority.
For example, Civil Service suitability investigations are conducted under Executive Order 10450. This is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and written inquiries to appropriate law enforcement agencies.

§ 20.21(b)(3).

This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§ 20.21(b)(4).

Under this subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in § 20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specifically “certification” criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

“Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action suit, or other judicial or administrative proceedings.”
LEAA anticipates issuing regulations, pursuant to section 524(a) as soon as possible.

§ 20.21(c)(2).

Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of invasion of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§ 20.21(c)(3).

The language of this subsection leaves to the States the question of who among the agencies and individuals listed in § 20.21(b) shall actually receive criminal records. Under these regulations a State could place a total ban on dissemination if it so wished. The State could, on the other hand, enact laws authorizing any member of the private sector to have access to non-conviction data.

§ 20.21(d).

Non-criminal justice agencies will not be able to receive records of juveniles unless the language of a statute or court order, rule, or court decision specifies that juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations for eligibility to classified information under existing legal authority.

§ 20.21(e)

Since it would be too costly to audit each criminal justice agency in most States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a “representative sample” of agencies are the next best alternative. The term “representative sample” is used to insure that audits do not simply focus on certain types of agencies. Although this subsection requires that there be records kept with the names of all persons or agencies to whom information is disseminated, criminal justice agencies are not required to maintain dissemination logs for “no record” responses.

§ 20.21(f).
Requirements are set forth which the States must meet in order to assure that criminal history record information is adequately protected. Automated systems may operate in shared environments and the regulations require certain minimum assurances.

§ 20.21(g)(1).

A “challenge” under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that States ought to be free to determine other means of identity verification.

§ 20.21(g)(5).

Not every agency will have done this in the past, but henceforth adequate records including those required under 20.21(e) must be kept so that notification can be made.

§ 20.21(g)(6).

This section emphasizes that the right to access and review extends only to criminal history record information and does not include other information such as intelligence or treatment data.

§ 20.22(a).

The purpose for the certification requirement is to indicate the extent of compliance with these regulations. The term “maximum extent feasible” acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

Note:
In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History
Information Systems, Technical Reports No. 2 and No. 13; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum No. 3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum No. 4.

Subpart C

§ 20.31.

This section defines the criminal history record information system managed by the Federal Bureau of Investigation. Each state having a record in the III System must have fingerprints on file in the FBI CJIS Division to support the III System record concerning the individual.

Paragraph (b) is not intended to limit the identification services presently performed by the FBI for local, state, tribal, and federal agencies.

§ 20.32.

The grandfather clause contained in paragraph (c) of this section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses that were stored prior to February, 1973. In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will also appear in the arrest segment of the III System record.

§ 20.33(a)(3).

This paragraph incorporates provisions cited in 28 CFR 50.12 regarding dissemination of identification records outside the federal government for noncriminal justice purposes.

§ 20.33(a)(6).

Noncriminal justice governmental agencies are sometimes tasked to perform criminal justice dispatching functions or data processing/information services for criminal justice agencies as part, albeit not a principal part, of their responsibilities. Although such inter-governmental delegated tasks involve the administration of criminal justice, performance of those tasks does not convert an otherwise non-criminal justice agency to a criminal justice agency. This regulation authorizes this type of delegation if it is effected pursuant to executive order, statute, regulation, or interagency agreement. In this context, the noncriminal justice agency is servicing the criminal justice agency by performing
an administration of criminal justice function and is permitted access to criminal history record information to accomplish that limited function. An example of such delegation would be the Pennsylvania Department of Administration's Bureau of Consolidated Computer Services, which performs data processing for several state agencies, including the Pennsylvania State Police. Privatization of the data processing/information services or dispatching function by the noncriminal justice governmental agency can be accomplished pursuant to § 20.33(a)(7) of this part.

§ 20.34.

The procedures by which an individual may obtain a copy of his manual identification record are set forth in 28 CFR 16.30-16.34.

The procedures by which an individual may obtain a copy of his III System record are as follows: If an individual has a criminal record supported by fingerprints and that record has been entered in the III System, it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and federal administrative and statutory regulations. Appropriate identification includes being fingerprinted for the purpose of insuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingerprints.

Procedure.
1. All requests for review must be made by the subject of the record through a law enforcement agency which has access to the III System. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI identification number of the individual's record is available to that agency, it can make an on-line inquiry through NCIC to obtain his III System record or, if it does not have suitable equipment to obtain an on-line response, obtain the record from Clarksburg, West Virginia, by mail. The individual will then be afforded the opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI, or, possibly, in the state's central identification agency.
4. The subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

§ 20.36.

This section refers to the requirements for obtaining direct access to the III System.

§ 20.37.

The 120-day requirement in this section allows 30 days more than the similar provision in subpart B in order to allow for processing time that may be needed by the states before forwarding the disposition to the FBI.

Official Citation:
28 CFR PART 21—WITNESS FEES

- 28 CFR Section 21.2: Employees of the United States serving as witnesses.
- 28 CFR Section 21.4: Fees and allowances of fact witnesses.
- 28 CFR Section 21.5: Use of table of distances.
- 28 CFR Section 21.7: Certification of witness attendance.

**Authority:**

**Source:**
51 FR 16171, May 1, 1986, unless otherwise noted.
28 CFR Section 21.1: Definitions.

(a) Agency proceeding.
An agency process as defined by 5 U.S.C. 551 (5), (7) and (9).

(b) Alien.
Any person who is not a citizen or national of the United States.

(c) Judicial proceeding.
Any action or suit, including any condemnation, preliminary, informational or other proceeding of a judicial nature. Examples of the latter include, but are not limited to, hearings and conferences before a committing court, magistrate, or commission, grand jury proceedings, pre-trial conferences, depositions, and coroners' inquests. It does not include information or investigative proceedings conducted by a prosecuting attorney for the purpose of determining whether an information or charge should be made in a particular case. The judicial proceeding may be in the District of Columbia, a State, or a territory or possession of the United States including the Commonwealth of Puerto Rico or the Trust Territory of the Pacific Islands.

(d) Pre-trial conference.
A conference between the Government Attorney and a witness to discuss the witness' testimony. The conference must take place after a trial, hearing or grand jury proceeding has been scheduled but prior to the witness' actual appearance at the proceeding.

(e) Residence.
The term residence is not limited to the legal residence, but includes any place at which the witness is actually residing and at which the subpoena or summons is served. If the residence of the witness at the time of appearance is different from the place of subpoena or summons, the new place of residence shall be considered the witness' residence for computation of the transportation allowance; but, if the witness is on a business or vacation trip at the time of appearance, the witness shall be paid for travel from the place of service if this does not result in the witness being paid for more travel than is actually performed.

(f) Summons.
An official request, invitation or call, evidenced by an official writing of the court, authority, or party responsible for the conduct of the proceeding.

28 CFR Section 21.2: Employees of the United States serving as witnesses.
(a) Applicability.
This section applies to employees of the United States as defined by 5 U.S.C. 2105, except those whose pay is disbursed by the Secretary of the Senate or the Clerk of the House of Representatives.

(b) Entitlement to travel expenses

(1) Official capacity.
An employee is entitled to travel expenses (in accordance with § 21.2(c)) in connection with any judicial or agency proceeding with respect to which the employee is summoned (and is authorized by the employee's agency to respond to such summons), or is assigned by his or her agency:

(i) To testify or produce official records on behalf of the United States, or

(ii) To testify in his or her official capacity or produce official records on behalf of a party other than the United States.

The witness appropriation of the Department of Justice is not available for expenses incurred under these conditions.

(2) Unofficial capacity, federal involvement.
An employee is entitled to travel expenses (in accordance with paragraph (c) of this section) in connection with any judicial or agency proceeding with respect to which the employee is summoned to testify on behalf of the United States. If an employee is summoned to testify on behalf of a party other than the United States, the employee's travel expenses shall be payable by the court, authority, or party which caused the employee to be summoned.

(3) Unofficial capacity, no Federal involvement.
An employee who appears as a witness in any judicial proceeding in an unofficial capacity in which there is no Federal involvement is not authorized Government travel expenses and may retain reimbursement for expenses which he or she receives from the court, authority or party which caused the employee to be summoned.

(c) Allowable travel expenses.
An employee qualifying for payment of travel expenses by virtue of being called in an official capacity or on behalf of the United States shall be paid at rates and in amounts allowable for other purposes under the provisions of 5 U.S.C. 5702-5705 and applicable regulations prescribed thereunder by the Administrator, General Services, and the employing agency. Such payment shall be reduced to the extent
that the travel expenses are paid to the employee for his or her appearance by the
court, authority, or party which caused the employee to be summoned as a
witness in an official capacity on behalf of a party other than the United States.

(d) Payment and reimbursement

(1) Payable by the employing agency.
If an employee serves as a witness, and the case involves the activity in
connection with which he or she is employed, the travel expenses are payable
from the appropriation of the employing agency. The Comptroller General has
defined the extent to which the case must be related to the agency’s activity as a
condition to the agency’s responsibility for payment in 23 Comp. Gen. 47, 49
(1943), which states “the employing agency is required to pay . . . the traveling
expenses incurred by the witness only where the information or facts ascertained
by the employee as part of his official duties forms the basis of the case, or where
the proceeding is predicated upon a law that that agency is required to
administer.” In 39 Comp. Gen. 1, 2 (1959), the Comptroller General determined
that if an employee testifies regarding facts and information he or she acquires in
the course of his or her assigned duties, the employing agency is responsible for
the payment of the employee’s travel expenses. In these instances, the witness
appropriation of the Department of Justice is not available for payment of
expenses.

(2) Payable by the Department of Justice.
If an employee appears on behalf of the United States in an unofficial capacity in
a judicial proceeding involving the Department of Justice, the employee’s travel
expenses are payable by the Department of Justice. The employing agency may
advance or pay the travel expenses of the employee and later obtain
reimbursement from the Department of Justice by submitting an appropriate bill
together with a copy of the approved advance or travel voucher.

(e) Leave and attendance fee

(1) Leave.
An employee is considered to be in official duty status when appearing as a
witness in his or her official capacity or on behalf of the United States in an
unofficial capacity. An employee is entitled to court leave when he or she appears
as a witness in an unofficial capacity not on behalf of the United States, and the
United States, the District of Columbia, or a State or local government is a party
to the case. An employee must use annual leave or leave without pay to appear as
a witness when the United States, the District of Columbia, or a State or local
government is not a party.
(2) Attendance fee.
An employee who appears on behalf of the United States is not entitled to receive an attendance fee. An employee who appears on behalf of a party other than the United States while in official duty status or while on court leave should request an attendance fee from the court, authority, or party which caused the employee to be summoned. Such fee shall be remitted to the employing agency. An employee who must use annual leave or leave without pay to appear as a witness may retain an attendance fee which he or she receives.

28 CFR Section 21.3: Aliens.

(a) Aliens entitled to payment of $30 per day.
The following aliens are entitled to witness fees and allowances provided in § 21.4:

(1) Aliens lawfully admitted for permanent residence (documentary evidence: Form I-151 or Form 1-551, Alien Registration Receipt Card);

(2) Aliens lawfully admitted in one of the nonimmigrant categories described in 8 U.S.C. 1101(a)(15) (documentary evidence: unexpired Form 1-94, Arrival-Departure Record). But see below § 21.3(b);


(4) Aliens who have rendered themselves amenable to deportation proceedings, but have not admitted deportability or have not been determined to be deportable pursuant to section 242 of the Immigration and Nationality Act (8 U.S.C. 1252).

(b) Aliens entitled to payment of $1 per day.
An alien who is “excludable” in accordance with 8 U.S.C. 1226, but whose removal is stayed by the Attorney General (in accordance with 8 U.S.C. 1227(d)) because:

(1) The testimony of the alien is necessary on behalf of the United States in the prosecution of offenders against the United States, or

(2) The testimony of the alien is necessary on behalf of an indigent criminal defendant in accordance with Rule 17(b) of the Federal Rules of Criminal Procedures,
is entitled to a $1 per day witness fee. No other fees and allowances are authorized.

(c) Aliens not entitled to payment.
An alien who has been paroled into the United States for prosecution pursuant to 8 U.S.C. 1182(d)(5) (documentary evidence: Form I-94, Arrival-Departure Record, Parole Edition), or an alien who has admitted belonging to a class of aliens who are deportable, or an alien who has been determined pursuant to 8 U.S.C. 1252(b) to be deportable (documentary evidence: decision by a Special Inquiry Officer, Board of Immigration Appeals, or court), is prohibited from receiving fees and allowances in accordance with 28 U.S.C. 1821(e).

(d) Doubtful cases.
If the Immigration and Naturalization Service advises that the alien has admitted deportability, or that he or she was paroled into the United States for prosecution, or that deportation proceedings have been completed against the alien with a result favorable to the Government, no payment under 28 U.S.C. 1821 may be made.

28 CFR Section 21.4: Fees and allowances of fact witnesses.
The fees and allowances of fact witnesses, other than those covered by § 21.2, attending at any judicial proceeding, shall be as follows:

(a) Fee.
A witness shall be paid an attendance fee of $30 per day for each day's attendance. A witness shall also be paid the attendance fee for the time necessarily occupied in going to and returning from the place of attendance. However, if both attendance and travel occur on the same day, a witness is entitled to only one fee.

(b) Allowable transportation expenses.
A witness shall be entitled to transportation expenses based on the means of transportation reasonably utilized (based on the nature, duration, location and distance of travel) and the distance necessarily traveled from and to such witness' residence by the shortest practical route and the fastest means of transportation available in going to and returning from the place of attendance. Additional costs incurred (including attendance fees and subsistence allowances) because of a slower means of transportation must be justified for consideration.

(1) A witness who travels by regularly scheduled common carrier shall be paid for the actual expenses of transportation at the most economical rate reasonably available. A receipt or other evidence of actual cost shall be furnished.
(2) A witness who travels by privately owned vehicle shall be paid a transportation allowance equal to the mileage allowance paid for official travel of employees of the Federal Government under the provisions of 5 U.S.C. 5704. However, when two or more witnesses travel in the same privately owned vehicle, only the witness incurring the expense shall receive the mileage allowance.

(3) A witness incurring incidental transportation expenses, such as taxi fares between the place of attendance, residence or lodging and the carrier terminals; bridge, road and tunnel tolls; ferry fares; and parking fees shall be paid in full for such expenses. Receipts or other evidence of actual payment are required for all parking fees (if available) and all other single items costing more than $25.

(4) First-class travel by witnesses requires the same justification and approval required for first-class travel by employees of the Federal Government.

c) Subsistence allowance. A witness (other than a witness detained in custody) who is required to be away from his or her residence overnight is entitled to a subsistence allowance. A witness who is not required to be away from his or her residence overnight is not entitled to a subsistence allowance. The witness' subsistence allowance shall not exceed either the per diem rate or the actual subsistence allowance rate prescribed for Government employees for the place of attendance. These rates are established by the Administrator, General Services, for areas within the conterminous United States; the Secretary of Defense for areas of the United States other than conterminous; or the Secretary of State as published in the Standardized Regulations (Government Civilians, Foreign Areas) for foreign areas. The witness' subsistence allowance shall consist of a meal and miscellaneous expense portion and a lodging portion. When an overnight stay is required, the witness shall be entitled to:

(1) The meal and miscellaneous expense portion for each day (or partial day) the witness is required to remain away from his or her residence and

(2) The lodging portion for each night the witness is required to incur a lodging expense.

The meal and miscellaneous expense portion shall be 50% of the authorized subsistence allowance rate rounded to the next whole dollar in an actual subsistence rate area, or 45% of the per diem rate rounded to the next whole dollar in a per diem area. The lodging portion shall be the difference between the meal and miscellaneous expense portion and the authorized rate.

d) Detained witness fee.
A witness (other than an alien covered by § 21.3) detained in custody pursuant to 18 U.S.C. 3149 for want of security for his or her appearance shall receive subsistence in kind and shall be paid a single daily attendance fee for each day the witness is detained. A witness in custody for purposes other than 18 U.S.C. 3149 is ineligible to receive the attendance and subsistence fees provided by this section.

28 CFR Section 21.5: Use of table of distances.

Mileage payable to witnesses under 28 U.S.C. 1821 shall be computed on the basis of odometer readings or the highway distances as stated in the Rand McNally Standard Highway Mileage Guide or in any generally accepted highway mileage guide which contains a shortline nationwide table of distances. However, with respect to travel in areas for which no such highway mileage guide exists, mileage payable under 28 U.S.C. 1821 shall be based on the lesser of either (a) the route of travel actually employed or (b) a usually traveled route.


Title 28 U.S.C. 1915 provides for the commencement, prosecution or defense of any suit, action, or proceeding without prepayment of fees and costs. Witnesses shall attend as in other cases.

(a) Civil cases.
There are currently no provisions for payment of witnesses called by the indigent. If the indigent party prevails, witness fees and expenses may be taxed as costs in accordance with 28 U.S.C. 1920.

(b) Criminal cases.
Rule 17(b), Federal Rules of Criminal Procedure, requires that fact witnesses subpoenaed on behalf of an indigent defendant be paid in the same manner as witnesses called on behalf of the Government. The attendance must be certified by the presiding officer of the court. The expenses of Federal Government employees are treated in the same manner as they are treated when the employee is called by a Government attorney.

28 CFR Section 21.7: Certification of witness attendance.

In any case in which the U.S. Department of Justice, or office or organization thereof, is a party, the Department of Justice shall pay all fees and allowances of
witnesses, except for those witnesses as defined in § 21.2, paragraph (d)(1), on the certification of the following officials: The U.S. Attorney, an Assistant U.S. Attorney, a U.S. Trustee, or the U.S. Department of Justice attorney who actually conducts the case. In criminal proceedings in forma pauperis or in proceedings before a U.S. Commissioner, U.S. Magistrate or U.S. Parole Commission Hearing Examiner, the Department of Justice shall pay all fees and allowances of witnesses on the certification of the U.S. District Judge hearing the case or such Commissioner, Magistrate, or Hearing Examiner.
28 CFR PART 22—CONFIDENTIALITY OF IDENTIFIABLE RESEARCH AND STATISTICAL INFORMATION

- 28 CFR Section 22.1: Purpose.
- 28 CFR Section 22.2: Definitions.
- 28 CFR Section 22.20: Applicability.
- 28 CFR Section 22.21: Use of identifiable data.
- 28 CFR Section 22.22: Revelation of identifiable data.
- 28 CFR Section 22.23: Privacy certification.
- 28 CFR Section 22.24: Information transfer agreement.
- 28 CFR Section 22.25: Final disposition of identifiable materials.
- 28 CFR Section 22.26: Requests for transfer of information.
- 28 CFR Section 22.27: Notification.
- 28 CFR Section 22.28: Use of data identifiable to a private person for judicial, legislative or administrative purposes.
- 28 CFR Section 22.29: Sanctions.

Authority:

Source:
41 FR 54846, Dec. 15, 1976, unless otherwise noted.
28 CFR Section 22.1: Purpose.

The purpose of these regulations is to:

(a) Protect privacy of individuals by requiring that information identifiable to a private person obtained in a research or statistical program may only be used and/or revealed for the purpose for which obtained;

(b) Insure that copies of such information shall not, without the consent of the person to whom the information pertains, be admitted as evidence or used for any purpose in any judicial or administrative proceedings;

(c) Increase the credibility and reliability of federally-supported research and statistical findings by minimizing subject concern over subsequent uses of identifiable information;

(d) Provide needed guidance to persons engaged in research and statistical activities by clarifying the purposes for which identifiable information may be used or revealed; and

(e) Insure appropriate balance between individual privacy and essential needs of the research community for data to advance the state of knowledge in the area of criminal justice.

(f) Insure the confidentiality of information provided by crime victims to crisis intervention counselors working for victim services programs receiving funds provided under the Crime Control Act, and Juvenile Justice Act, and the Victims of Crime Act.

Official Citation:

28 CFR Section 22.2: Definitions.

(a) Person
means any individual, partnership, corporation, association, public or private organization or governmental entity, or combination thereof.

(b) Private person
means any person defined in § 22.2(a) other than an agency, or department of Federal, State, or local government, or any component or combination thereof. Included as a private person is an individual acting in his or her official capacity.

(c) Research or statistical project
means any program, project, or component thereof which is supported in whole or in part with funds appropriated under the Act and whose purpose is to develop, measure, evaluate, or otherwise advance the state of knowledge in a particular area. The term does not include “intelligence” or other information-gathering activities in which information pertaining to specific individuals is obtained for purposes directly related to enforcement of the criminal laws.

(d) Research or statistical information means any information which is collected during the conduct of a research or statistical project and which is intended to be utilized for research or statistical purposes. The term includes information which is collected directly from the individual or obtained from any agency or individual having possession, knowledge, or control thereof.

(e) Information identifiable to a private person means information which either—

(1) Is labelled by name or other personal identifiers, or

(2) Can, by virtue of sample size or other factors, be reasonably interpreted as referring to a particular private person.

(f) Recipient of assistance means any recipient of a grant, contract, interagency agreement, subgrant, or subcontract under the Act and any person, including subcontractors, employed by such recipient in connection with performances of the grant, contract, or interagency agreement.

(g) Officer or employee of the Federal Government means any person employed as a regular or special employee of the U.S. (including experts, consultants, and advisory board members) as of July 1, 1973, or at any time thereafter.


(i) Applicant means any person who applies for a grant, contract, or subgrant to be funded pursuant to the Act.


Official Citation:

28 CFR Section 22.20: Applicability.

(a) These regulations govern use and revelation of research and statistical information obtained, collected, or produced either directly by BJA, OJJDP, BJS, NIJ, or OJP or under any interagency agreement, grant, contract, or subgrant awarded under the Crime Control Act, the Juvenile Justice Act, and the Victims of Crime Act.

(b) The regulations do not apply to any records from which identifiable research or statistical information was originally obtained; or to any records which are designated under existing statutes as public; or to any information extracted from any records designated as public.

(c) The regulations do not apply to information gained regarding future criminal conduct.

Official Citation:

28 CFR Section 22.21: Use of identifiable data.

Research or statistical information identifiable to a private person may be used only for research or statistical purposes.

28 CFR Section 22.22: Revelation of identifiable data.

(a) Except as noted in paragraph (b) of this section, research and statistical information relating to a private person may be revealed in identifiable form on a need-to-know basis only to—

(1) Officers, employees, and subcontractors of the recipient of assistance;
(2) Such individuals as needed to implement sections 202(c)(3), 801, and 811(b) of the Act; and sections 223(a)(12)(A), 223(a)(13), 223(a)(14), and 243 of the Juvenile Justice and Delinquency Prevention Act.

(3) Persons or organizations for research or statistical purposes. Information may only be transferred for such purposes upon a clear demonstration that the standards of § 22.26 have been met and that, except where information is transferred under paragraphs (a)(1) and (2) of this section, such transfers shall be conditioned on compliance with a § 22.24 agreement.

(b) Information may be revealed in identifiable form where prior consent is obtained from an individual or where the individual has agreed to participate in a project with knowledge that the findings cannot, by virtue of sample size, or uniqueness of subject, be expected to totally conceal subject identity.

Official Citation:

28 CFR Section 22.23: Privacy certification.

(a) Each applicant for BJA, OJJDP, BJS, NIJ, or OJP support either directly or under a State plan shall submit a Privacy Certificate as a condition of approval of a grant application or contract proposal which has a research or statistical project component under which information identifiable to a private person will be collected.

(b) The Privacy Certificate shall briefly describe the project and shall contain assurance by the applicant that:

1. Data identifiable to a private person will not be used or revealed, except as authorized under §§ 22.21, 22.22.

2. Access to data will be limited to those employees having a need therefore and that such persons shall be advised of and agree in writing to comply with these regulations.

3. All subcontracts which require access to identifiable data will contain conditions meeting the requirements of § 22.24.

4. To the extent required by § 22.27 any private persons from whom identifiable data are collected or obtained, either orally or by means of written questionnaire, shall be advised that the data will only be used or revealed for research or statistical purposes and that compliance with requests for information is not mandatory. Where the notification requirement is to be
waived, pursuant to § 22.27(c), a justification must be included in the Privacy Certificate.

(5) Adequate precautions will be taken to insure administrative and physical security of identifiable data.

(6) A log will be maintained indicating that identifiable data have been transmitted to persons other than BJA, OJJDP, BJS, NIJ, or OJP or grantee/contractor staff or subcontractors, that such data have been returned, or that alternative arrangements have been agreed upon for future maintenance of such data.

(7) Project plans will be designed to preserve anonymity of private persons to whom information relates, including, where appropriate, name-stripping, coding of data, or other similar procedures.

(8) Project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person except as authorized under § 22.22.

(c) The applicant shall attach to the Privacy Certification a description of physical and/or administrative procedures to be followed to insure the security of the data to meet the requirements of § 22.25.

**Official Citation:**

**28 CFR Section 22.24: Information transfer agreement.**

Prior to the transfer of any identifiable information to persons other than BJA, OJJDP, BJS, NIJ, or OJP or project staff, an agreement shall be entered into which shall provide, as a minimum, that the recipient of data agrees that:

(a) Information identifiable to a private person will be used only for research and statistical purposes.

(b) Information identifiable to a private person will not be revealed to any person for any purpose except where the information has already been included in research findings (and/or data bases) and is revealed on a need-to-know basis for research or statistical purposes, provided that such transfer is approved by the person providing information under the agreement, or authorized under § 22.24(e).
(c) Knowingly and willfully using or disseminating information contrary to the provisions of the agreement shall constitute a violation of these regulations, punishable in accordance with the Act.

(d) Adequate administrative and physical precautions will be taken to assure security of information obtained for such purpose.

(e) Access to information will be limited to those employees or subcontractors having a need therefore in connection with performance of the activity for which obtained, and that such persons shall be advised of, and agree to comply with, these regulations.

(f) Project plans will be designed to preserve anonymity of private persons to whom information relates, including, where appropriate, required name-stripping and/or coding of data or other similar procedures.

(g) Project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person.

(h) Information identifiable to a private person (obtained in accordance with this agreement) will, unless otherwise agreed upon, be returned upon completion of the project for which obtained and no copies of that information retained.

Official Citation:

28 CFR Section 22.25: Final disposition of identifiable materials.

Upon completion of a research or statistical project the security of identifiable research or statistical information shall be protected by:

(a) Complete physical destruction of all copies of the materials or the identifiable portion of such materials after a three-year required recipient retention period or as soon as authorized by law, or

(b) Removal of identifiers from data and separate maintenance of a name-code index in a secure location.

The Privacy Certificate shall indicate the procedures to be followed and shall, in the case of paragraph (b) of this section, describe procedures to secure the name index.
28 CFR Section 22.26: Requests for transfer of information.

(a) Requests for transfer of information identifiable to an individual shall be submitted to the person submitting the Privacy Certificate pursuant to § 22.23.

(b) Except where information is requested by BJA, OJJDP, BJS, NIJ, or OJP, the request shall describe the general objectives of the project for which information is requested, and specifically justify the need for such information in identifiable form. The request shall also indicate, and provide justification for the conclusion that conduct of the project will not, either directly or indirectly, cause legal, economic, physical, or social harm to individuals whose identification is revealed in the transfer of information.

(c) Data may not be transferred pursuant to this section where a clear showing of the criteria set forth above is not made by the person requesting the data.

Official Citation:

28 CFR Section 22.27: Notification.

(a) Any person from whom information identifiable to a private person is to be obtained directly, either orally, by questionnaire, or other written documents, shall be advised:

   (1) That the information will only be used or revealed for research or statistical purposes; and

   (2) That compliance with the request for information is entirely voluntary and may be terminated at any time.

(b) Except as noted in paragraph (c) of this section, where information is to be obtained through observation of individual activity or performance, such individuals shall be advised:

   (1) Of the particular types of information to be collected;

   (2) That the data will only be utilized or revealed for research or statistical purposes; and

   (3) That participation in the project in question is voluntary and may be terminated at any time.
(c) Notification, as described in paragraph (b) of this section, may be eliminated where information is obtained through field observation of individual activity or performance and in the judgment of the researcher such notification is impractical or may seriously impede the progress of the research.

(d) Where findings in a project cannot, by virtue of sample size, or uniqueness of subject, be expected to totally conceal subject identity, an individual shall be so advised.

28 CFR Section 22.28: Use of data identifiable to a private person for judicial, legislative or administrative purposes.

(a) Research or statistical information identifiable to a private person shall be immune from legal process and shall only be admitted as evidence or used for any purpose in any action, suit, or other judicial, legislative or administrative proceeding with the written consent of the individual to whom the data pertains.

(b) Where consent is obtained, such consent shall:

(1) Be obtained at the time that information is sought for use in judicial, legislative or administrative proceedings;

(2) Set out specific purposes in connection with which information will be used;

(3) Limit, where appropriate, the scope of the information subject to such consent.

Official Citation:

28 CFR Section 22.29: Sanctions.

Where BJA, OJJDP, BJS, NIJ, or OJP believes that a violation of section 812(a) of the Act or section 1407(d) of the Victims of Crime Act, these regulations, or any grant or contract conditions entered into thereunder has occurred, it may initiate administrative actions leading to termination of a grant or contract, commence appropriate personnel and/or other procedures in cases involving Federal employees, and/or initiate appropriate legal actions leading to imposition of a civil penalty not to exceed $10,000 for a violation occurring before September 29,
1999, and not to exceed $11,000 for a violation occurring on or after September 29, 1999 against any person responsible for such violations.

**Official Citation:**
[Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]
28 CFR PART 23—CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

- 28 CFR Section 23.1: Purpose.
- 28 CFR Section 23.2: Background.
- 28 CFR Section 23.3: Applicability.
- 28 CFR Section 23.20: Operating principles.
- 28 CFR Section 23.30: Funding guidelines.
- 28 CFR Section 23.40: Monitoring and auditing of grants for the funding of intelligence systems.

Authority:
42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

Source:
58 FR 48452, Sept. 16, 1993, unless otherwise noted.
28 CFR Section 23.1: Purpose.


28 CFR Section 23.2: Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

28 CFR Section 23.3: Applicability.


(b) As used in these policies:

(1) Criminal Intelligence System or Intelligence System

means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information;
(2) Interjurisdictional Intelligence System

means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions;

(3) Criminal Intelligence Information

means data which has been evaluated to determine that it:

(i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and

(ii) Meets criminal intelligence system submission criteria;

(4) Participating Agency

means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system;

(5) Intelligence Project or Project

means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and

(6) Validation of Information

means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

28 CFR Section 23.20: Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual
is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f)(1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.
(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

1. Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

2. The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

3. The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

4. The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

5. The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

6. A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for
continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(ii) [Reserved]

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.
(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

28 CFR Section 23.30: Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d)(1) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with
general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(i) Assume official responsibility and accountability for actions taken in the name of the joint entity, and

(ii) Certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

(2) The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

28 CFR Section 23.40: Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR part 23 Criminal Intelligence Systems Policies.
Subpart A—General Provisions
- 28 CFR Section 24.101: Purpose of these rules.
- 28 CFR Section 24.102: Definitions.
- 28 CFR Section 24.104: Applicability to Department of Justice proceedings.

Subpart B—Information Required From Applicants
- 28 CFR Section 24.201: Contents of application.
- 28 CFR Section 24.203: Documentation of fees and expenses.
- 28 CFR Section 24.204: Time for submission of application.

Subpart C—Procedures for Considering Applications
- 28 CFR Section 24.302: Answer to application.
- 28 CFR Section 24.303: Comments by other parties.
- 28 CFR Section 24.305: Extensions of time.
- 28 CFR Section 24.306: Decision on application.
- 28 CFR Section 24.307: Department review.
- 28 CFR Section 24.309: Payment of award.

Authority:
5 U.S.C. 504(c)(1).

Source:
Order No. 975-82, 47 FR 15776, Apr. 13, 1982, unless otherwise noted.
SUBPART A—General Provisions

28 CFR Section 24.101: Purpose of these rules.

These rules are adopted by the Department of Justice pursuant to section 504 of title 5, U.S. Code, as amended by section 203(a)(1) of the Equal Access to Justice Act, Public Law No. 96-481. Under the Act, an eligible party may receive an award for attorney fees and other expenses when it prevails over the Department in an adversary adjudication under 5 U.S.C. 554 before the Department, unless the Department's position as a party to the proceeding was substantially justified or special circumstances make an award unjust. The purpose of these rules is to establish procedures for the submission and consideration of applications for awards against the Department.

28 CFR Section 24.102: Definitions.

As used in this part:

(a) The Act
means section 504 of title 5, U.S. Code, as amended by section 203(a)(1) of the Equal Access to Justice Act, Public Law No. 96-481.

(b) Adversary adjudication
means an adjudication under 5 U.S.C. 554 in which the position of the United States is represented by counsel or otherwise, but excludes an adjudication for the purpose of establishing or fixing a rate or for the purpose of granting or reviewing a license.

(c) Adjudicative officer
means the official, without regard to whether the official is designated as an administrative law judge, a hearing officer or examiner, or otherwise, who presided at the adversary adjudication.

(d) Department
refers to the relevant departmental component which is conducting the adversary adjudication (e.g., Drug Enforcement Administration or Office of Justice Assistance, Research, and Statistics).

(e) Proceeding
means an adversary adjudication as defined in § 24.102(b) above.

(a) These rules apply to adversary adjudications required by statute to be conducted by the Department under 5 U.S.C. 554. Specifically, the proceedings conducted by the Department to which these rules apply are:

(1) Hearings conducted by the Drug Enforcement Administration (DEA) in connection with suspension or revocation of registration of manufacturers, distributors, and dispensers of controlled substances under 21 U.S.C. 824(c) and 21 CFR 1301.51; suspension or revocation of import and export registrations pursuant to 21 U.S.C. 958 and 21 CFR 1311.51;

(2) Hearings conducted by DEA in connection with the scheduling of drugs pursuant to 21 U.S.C. 811(a) and 21 CFR 1308.41;

(3) Handicap discrimination hearings conducted by the Department under 29 U.S.C. 794a(a) and 28 CFR 42.109(d);

(4) Title VI civil rights hearings conducted by the Department under 42 U.S.C. 2000d-1 and 28 CFR 42.109(d);

(5) Grant denial and grant termination hearings conducted by the Office of Justice Assistance, Research, and Statistics (OJARS), the National Institute of Justice (NIJ), the Bureau of Justice Statistics (BJS) and the Office of Juvenile Justice and Delinquency Prevention (OJJDP), or the Law Enforcement Assistance Administration (LEAA) under 42 U.S.C. 3783 and 28 CFR part 18; and


(b) If a proceeding includes both matters covered by the Act and matters specifically excluded from coverage, any award made will include only fees and expenses related to covered issues.

28 CFR Section 24.104: Applicability to Department of Justice proceedings.

The Act applies to an adversary adjudication pending before the Department at any time between October 1, 1981 and September 30, 1984. This includes proceedings begun before October 1, 1981 if final Department action has not been taken before that date, and proceedings pending on September 30, 1984.
28 CFR Section 24.105: Eligibility of applicants.

(a) To be eligible for an award of attorney fees and other expenses under the Act, the applicant must be a prevailing party in the adversary adjudication for which it seeks an award. The term “party” is defined in 5 U.S.C. 551(3). The applicant must show that it meets all conditions of eligibility set out in this subpart and in subpart B.

(b) The types of eligible applicants are as follows:

(1) An individual with a net worth of not more than $1 million;

(2) The sole owner of an unincorporated business who has a net worth of not more than $5 million and not more than 500 employees;

(3) A charitable or other tax-exempt organization described in section 501(c)(3) of the Internal Revenue Code (26 U.S.C. 501(c)(3)) with not more than 500 employees;

(4) A cooperative association as defined in section 15(a) of the Agricultural Marketing Act (12 U.S.C. 1141j(a)) with not more than 500 employees; and

(5) Any other partnership, corporation, association, or public or private organization with a net worth of not more than $5 million and not more than 500 employees.

(c) For the purpose of eligibility, the net worth and number of employees of an applicant shall be determined as of the date the adversary adjudication was initiated.

28 CFR Section 24.106: Standards for awards.

(a) A prevailing applicant may receive an award for fees and expenses incurred in connection with a proceeding unless (1) the position of the Department as a party to the proceeding was substantially justified or (2) special circumstances make the award sought unjust. No presumption arises that the agency's position was not substantially justified simply because the agency did not prevail.

(b) An award will be reduced or denied if the applicant has unduly or unreasonably protracted the proceedings.
(a) The following fees and other expenses are allowable under the Act:

    (1) Reasonable expenses of expert witnesses;

    (2) Reasonable cost of any study, analysis, engineering report, test, or project which the Department finds necessary for the preparation of the party's case;

    (3) Reasonable attorney or agent fees;

(b) The amount of fees awarded will be based upon the prevailing market rates for the kind and quality of services furnished, except that

    (1) Compensation for an expert witness will not exceed the highest rate paid by the Department for expert witnesses; and

    (2) Attorney or agent fees will not be in excess of $75 per hour.
SUBPART B—Information Required From Applicants
28 CFR Section 24.201: Contents of application.

(a) An application for an award of fees and expenses under the Act shall identify the applicant and the proceeding for which an award is sought. The application shall show that the applicant has prevailed and identify the position of the Department in the proceeding that the applicant alleges was not substantially justified.

(b) The application shall include a statement that the applicant’s net worth as of the time the proceeding was initiated did not exceed $1 million if the applicant is an individual (other than a sole owner of an unincorporated business seeking an award in that capacity) or $5 million in the case of all other applicants. An applicant may omit this statement if:

(1) It attaches a copy of a ruling by the Internal Revenue Service that it qualifies as an organization described in section 501(c)(3) of the Internal Revenue Code of 1954 (26 U.S.C. 501(c)(3)) and is exempt from taxation under section 501(a) of the Code or, in the case of such an organization not required to obtain a ruling from the Internal Revenue Service on its exempt status, a statement that describes the basis for the applicant’s belief that it qualifies under section 501(c)(3) of the Code; or

(2) It states that it is a cooperative association as defined in section 15(a) of the Agricultural Marketing Act (12 U.S.C. 1141j(a)).

(c) If the applicant is a partnership, corporation, association, or organization, or a sole owner of an unincorporated business, the application shall state that it did not have more than 500 employees at the time the proceeding was initiated, giving the number of its employees and describing briefly the type and purpose of its organization or business.

(d) The application shall itemize the amount of fees and expenses for which an award is sought.

(e) The application may include any other matters that the applicant believes should be considered in determining whether and in what amount an award should be made.

(f) The application shall be signed by the applicant with respect to the eligibility of the applicant and by the attorney of the applicant with respect to fees and expenses sought. The application shall contain or be accompanied by a written verification under oath or affirmation under penalty of perjury that the information provided in the application and all accompanying material is true and complete to the best of the signer’s information and belief.

(a) Each applicant except a qualified tax exempt organization or a qualified cooperative must submit with its application a detailed exhibit showing its net worth at the time the proceeding was initiated. If any individual, corporation, or other entity directly or indirectly controls or owns a majority of the voting shares or other interest of the applicant, or if the applicant directly or indirectly owns or controls a majority of the voting shares of other interest of any corporation or other entity, the exhibit must include a showing of the net worth of all such affiliates or of the applicant including the affiliates. The exhibit may be in any form convenient to the applicant, provided that it makes full disclosure of the applicant's and any affiliates' assets and liabilities and is sufficient to determine whether the applicant qualifies under the standards of 5 U.S.C. 504(b)(1)(B)(i). The adjudicative officer may require an applicant to file additional information to determine the applicant's eligibility for an award.

(b) The net worth exhibit shall describe any transfers of assets from, or obligations incurred by, the applicant or any affiliate, occurring in the one-year period prior to the date on which the proceeding was initiated, that reduced the net worth of the applicant and its affiliates below the applicable net worth ceiling. If there were no such transactions, the applicant shall so state.

(c) The net worth exhibit shall be included in the public record of the proceeding.

28 CFR Section 24.203: Documentation of fees and expenses.

(a) The application shall be accompanied by full documentation of the fees and expenses, including the cost of any study, engineering report, test, or project, for which an award is sought.

(b) The documentation shall include an affidavit from any attorney, agent, or expert witness representing or appearing in behalf of the party, stating the actual time expended and the rate at which fees and other expenses were computed and describing the specific services performed.

   (1) The affidavit shall state the services performed. In order to establish the hourly rate, the affidavit shall state the hourly rate which is billed and paid by the majority of clients during the relevant time periods.

   (2) If no hourly rate is paid by the majority of clients because, for instance, the attorney or agent represents most clients on a contingency basis, the attorney
or agent shall provide information about two attorneys or agents with similar experience, who perform similar work, stating their hourly rate.

(c) The documentation shall also include a description of any expenses for which reimbursement is sought and a statement of the amounts paid and payable by the applicant or by any other person or entity for the services provided.

(d) The adjudicative officer may require the applicant to provide vouchers, receipts, or other substantiation for any expenses claimed.

28 CFR Section 24.204: Time for submission of application.

(a) An application must be filed no later than 30 days after final disposition of the proceeding. If review or reconsideration is sought or taken of a decision as to which an applicant believes it has prevailed, action on the award of fees shall be stayed pending final disposition of the underlying controversy.

(b) Final disposition means the later of:

(1) The date on which the final agency decision is issued,

(2) The date on which a petition for rehearing or reconsideration is disposed of, or

(3) The date of final resolution of the proceeding, such as settlement or voluntary dismissal, which is not subject to a petition for rehearing or reconsideration.
SUBPART C—Procedures for Considering Applications
28 CFR Section 24.301: Filing and service of documents.

An application for an award and any other pleading or document related to the application shall be filed and served on all parties to the proceeding in the same manner as other pleadings in the proceeding.

28 CFR Section 24.302: Answer to application.

(a) Within 30 calendar days after service of the application, Department counsel may file an answer. If Department counsel fails to answer or otherwise fails to contest or settle the application, the adjudicative officer may upon a satisfactory showing of entitlement by the applicant make an award for the applicant's fees and other expenses under 5 U.S.C. 504.

(b) If Department counsel and applicant believe that they can reach a settlement concerning the award, Department counsel may file a statement of intent to negotiate. The filing of such a statement shall extend the time for filing an answer an additional 30 days.

(c) The answer shall explain in detail any objections to the award requested and identify the facts relied on to support the objection. If the answer is based on any alleged facts not already reflected in the record of the proceeding, Department counsel shall include with the answer either a supporting affidavit or a request for further filings or other action.

28 CFR Section 24.303: Comments by other parties.

Any party to a proceeding other than the applicant and Department counsel may file comments on an application within 30 calendar days after it is served or on an answer within 15 calendar days after it is served.


A prevailing party and Department counsel may agree on a proposed settlement of an award before final action on the application, either in connection with a settlement of the underlying proceeding or after the underlying proceeding has been concluded. If the party and Department counsel agree on a proposed
settlement of an award before an application has been filed, the application shall be filed with the proposed settlement.

28 CFR Section 24.305: Extensions of time.

(a) The adjudicative officer may on motion and for good cause shown grant extensions of time other than for filing an application for fees and expenses after final disposition in the adversary adjudication.

(b) Ordinarily, the determination of an award will be made on the basis of the written record of the underlying proceeding and the filings required or permitted by the foregoing sections of these rules. However, the adjudicative officer may sua sponte or on motion of any party to the proceedings require or permit further filings or other action, such as an informal conference, oral argument, additional written submissions, or an evidentiary hearing. Such further action shall occur only when necessary for full and fair resolution of the issues arising from the application and shall take place as promptly as possible. A motion for further filings or other action shall specifically identify the information sought on the disputed issues and shall explain why the further filings or other action is necessary to resolve the issues.

(c) In the event that an evidentiary hearing is required or permitted by the adjudicative officer, such hearing and any related filings or other action required or permitted shall be conducted pursuant to the procedural rules governing adversary adjudications conducted by the Department component in which the underlying adversary adjudication was conducted.

28 CFR Section 24.306: Decision on application.

The adjudicative officer shall promptly issue a decision on the application which shall include proposed written findings and conclusions on such of the following as are relevant to the decision:

(a) The applicant’s status as a prevailing party;

(b) The applicant’s qualification as a “party” under 5 U.S.C. 504(b)(1)(B);

(c) Whether the Department’s position as a party to the proceeding was substantially justified;

(d) Whether special circumstances make an award unjust;
(e) Whether the applicant during the course of the proceedings engaged in conduct that unduly and unreasonably protracted the final resolution of the matter in controversy; and

(f) The amounts, if any, awarded for fees and other expenses, with reasons for any difference between the amount requested and the amount awarded.

**28 CFR Section 24.307: Department review.**

The decision of the adjudicative officer will be reviewed to the extent permitted by law by the Department in accordance with the Department’s procedures for the type of proceeding involved. The Department will issue the final decision on the application.

**28 CFR Section 24.308: Judicial review.**

Judicial review of final Department decisions on awards may be sought as provided in 5 U.S.C. 504(c)(2).

**28 CFR Section 24.309: Payment of award.**

An applicant seeking payment of an award shall submit a copy of the final decision granting the award to the Department's Accounting Office for processing. A statement that review of the underlying decision is not being sought in the United States courts, or that the process for seeking review of the award has been completed, must also be included.
Subpart A—The National Instant Criminal Background Check System
  o 28 CFR Section 25.1: Purpose and authority.
  o 28 CFR Section 25.2: Definitions.
  o 28 CFR Section 25.3: System information.
  o 28 CFR Section 25.4: Record source categories.
  o 28 CFR Section 25.5: Validation and data integrity of records in the system.
  o 28 CFR Section 25.6: Accessing records in the system.
  o 28 CFR Section 25.7: Querying records in the system.
  o 28 CFR Section 25.8: System safeguards.
  o 28 CFR Section 25.9: Retention and destruction of records in the system.
  o 28 CFR Section 25.10: Correction of erroneous system information.
  o 28 CFR Section 25.11: Prohibited activities and penalties.

Subpart B—National Motor Vehicle Title Information System (NMVTIS)
  o 28 CFR Section 25.51: Purpose and authority.
  o 28 CFR Section 25.52: Definitions.
  o 28 CFR Section 25.53: Responsibilities of the operator of NMVTIS.
  o 28 CFR Section 25.54: Responsibilities of the States.
  o 28 CFR Section 25.55: Responsibilities of insurance carriers.
  o 28 CFR Section 25.56: Responsibilities of junk yards and salvage yards and auto recyclers.
  o 28 CFR Section 25.57: Erroneous junk or salvage reporting.

Authority:

Source:
Order No. 2186-98, 63 FR 58307, Oct. 30, 1998, unless otherwise noted.
The purpose of this subpart is to establish policies and procedures implementing the Brady Handgun Violence Prevention Act (Brady Act), Public Law 103-159, 107 Stat. 1536. The Brady Act requires the Attorney General to establish a National Instant Background Check System (NICS) to be contacted by any licensed importer, licensed manufacturer, or licensed dealer of firearms for information as to whether the transfer of a firearm to any person who is not licensed under 18 U.S.C. 923 would be in violation of Federal or state law. The regulations in this subpart are issued pursuant to section 103(h) of the Brady Act, 107 Stat. 1542 (18 U.S.C. 922 note), and include requirements to ensure the privacy and security of the NICS and appeals procedures for persons who have been denied the right to obtain a firearm as a result of a NICS background check performed by the Federal Bureau of Investigation (FBI) or a state or local law enforcement agency.

**28 CFR Section 25.2: Definitions.**

Appeal means a formal procedure to challenge the denial of a firearm transfer.

ARI means a unique Agency Record Identifier assigned by the agency submitting records for inclusion in the NICS Index.

ATF means the Bureau of Alcohol, Tobacco, and Firearms of the Department of Treasury.

Audit log means a chronological record of system (computer) activities that enables the reconstruction and examination of the sequence of events and/or changes in an event.

Business day means a 24-hour day (beginning at 12:01 a.m.) on which state offices are open in the state in which the proposed firearm transaction is to take place.
Control Terminal Agency
means a state or territorial criminal justice agency recognized by the FBI as the agency responsible for providing state-or territory-wide service to criminal justice users of NCIC data.

Data source
means an agency that provided specific information to the NICS.

Delayed
means the response given to the FFL indicating that the transaction is in an “Open” status and that more research is required prior to a NICS “Proceed” or “Denied” response. A “Delayed” response to the FFL indicates that it would be unlawful to transfer the firearm until receipt of a follow-up “Proceed” response from the NICS or the expiration of three business days, whichever occurs first.

Denied
means denial of a firearm transfer based on a NICS response indicating one or more matching records were found providing information demonstrating that receipt of a firearm by a prospective transferee would violate 18 U.S.C. 922 or state law.

Denying agency
means a POC or the NICS Operations Center, whichever determines that information in the NICS indicates that the transfer of a firearm to a person would violate Federal or state law, based on a background check.

Dial-up access
means any routine access through commercial switched circuits on a continuous or temporary basis.

Federal agency
means any authority of the United States that is an “Agency” under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(10).

FFL (federal firearms licensee)
means a person licensed by the ATF as a manufacturer, dealer, or importer of firearms.

Firearm
has the same meaning as in 18 U.S.C. 921(a)(3).

Licensed dealer
means any person defined in 27 CFR 178.11.

Licensed importer
has the same meaning as in 27 CFR 178.11.

Licensed manufacturer
has the same meaning as in 27 CFR 178.11.

NCIC (National Crime Information Center)
means the nationwide computerized information system of criminal justice data established by the FBI as a service to local, state, and Federal criminal justice agencies.

NICS
means the National Instant Criminal Background Check System, which an FFL must, with limited exceptions, contact for information on whether receipt of a firearm by a person who is not licensed under 18 U.S.C. 923 would violate Federal or state law.

NICS Index
means the database, to be managed by the FBI, containing information provided by Federal and state agencies about persons prohibited under Federal law from receiving or possessing a firearm. The NICS Index is separate and apart from the NCIC and the Interstate Identification Index (III).

NICS operational day
means the period during which the NICS Operations Center has its daily regular business hours.

NICS Representative

Page 580
means a person who receives telephone inquiries to the NICS Operations Center from FFLs requesting background checks and provides a response as to whether the receipt or transfer of a firearm may proceed or is delayed.

NRI (NICS Record Identifier)
means the system-generated unique number associated with each record in the NICS Index.

NTN (NICS Transaction Number)
means the unique number that will be assigned to each valid background check inquiry received by the NICS. Its primary purpose will be to provide a means of associating inquiries to the NICS with the responses provided by the NICS to the FFLs.

Open
means those non-canceled transactions where the FFL has not been notified of the final determination. In cases of “open” responses, the NICS continues researching potentially prohibiting records regarding the transferee and, if definitive information is obtained, communicates to the FFL the final determination that the check resulted in a proceed or a deny. An “open” response does not prohibit an FFL from transferring a firearm after three business days have elapsed since the FFL provided to the system the identifying information about the prospective transferee.

ORI (Originating Agency Identifier)
means a nine-character identifier assigned by the FBI to an agency that has met the established qualifying criteria for ORI assignment to identify the agency in transactions on the NCIC System.

Originating Agency
means an agency that provides a record to a database checked by the NICS.

POC (Point of Contact)
means a state or local law enforcement agency serving as an intermediary between an FFL and the federal databases checked by the NICS. A POC will receive NICS background check requests from FFLs, check state or local record systems, perform NICS inquiries, determine whether matching records provide information demonstrating that an individual is disqualified from possessing a firearm under Federal or state law, and respond to FFLs with the results of a NICS background check. A POC will be an agency with express or implied
authority to perform POC duties pursuant to state statute, regulation, or executive order.

Proceed means a NICS response indicating that the information available to the system at the time of the response did not demonstrate that transfer of the firearm would violate federal or state law. A “Proceed” response would not relieve an FFL from compliance with other provisions of Federal or state law that may be applicable to firearms transfers. For example, under 18 U.S.C. 922(d), an FFL may not lawfully transfer a firearm if he or she knows or has reasonable cause to believe that the prospective recipient is prohibited by law from receiving or possessing a firearm.

Record means any item, collection, or grouping of information about an individual that is maintained by an agency, including but not limited to information that disqualifies the individual from receiving a firearm, and that contains his or her name or other personal identifiers.

STN (State-Assigned Transaction Number) means a unique number that may be assigned by a POC to a valid background check inquiry.

System means the National Instant Criminal Background Check System (NICS).

Official Citation:

28 CFR Section 25.3: System information.

(a) There is established at the FBI a National Instant Criminal Background Check System.

(b) The system will be based at the Federal Bureau of Investigation, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306-0147.

(c) The system manager and address are: Director, Federal Bureau of Investigation, J. Edgar Hoover F.B.I. Building, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535.
It is anticipated that most records in the NICS Index will be obtained from Federal agencies. It is also anticipated that a limited number of authorized state and local law enforcement agencies will voluntarily contribute records to the NICS Index. Information in the NCIC and III systems that will be searched during a background check has been or will be contributed voluntarily by Federal, state, local, and international criminal justice agencies.

(a) The FBI will be responsible for maintaining data integrity during all NICS operations that are managed and carried out by the FBI. This responsibility includes:

(1) Ensuring the accurate adding, canceling, or modifying of NICS Index records supplied by Federal agencies;

(2) Automatically rejecting any attempted entry of records into the NICS Index that contain detectable invalid data elements;

(3) Automatic purging of records in the NICS Index after they are on file for a prescribed period of time; and

(4) Quality control checks in the form of periodic internal audits by FBI personnel to verify that the information provided to the NICS Index remains valid and correct.

(b) Each data source will be responsible for ensuring the accuracy and validity of the data it provides to the NICS Index and will immediately correct any record determined to be invalid or incorrect.

(a) FFLs may initiate a NICS background check only in connection with a proposed firearm transfer as required by the Brady Act. FFLs are strictly prohibited from initiating a NICS background check for any other purpose. The process of
accessing the NICS for the purpose of conducting a NICS background check is initiated by an FFL's contacting the FBI NICS Operations Center (by telephone or electronic dial-up access) or a POC. FFLs in each state will be advised by the ATF whether they are required to initiate NICS background checks with the NICS Operations Center or a POC and how they are to do so.

(b) Access to the NICS through the FBI NICS Operations Center. FFLs may contact the NICS Operations Center by use of a toll-free telephone number, only during its regular business hours. In addition to telephone access, toll-free electronic dial-up access to the NICS will be provided to FFLs after the beginning of the NICS operation. FFLs with electronic dial-up access will be able to contact the NICS 24 hours each day, excluding scheduled and unscheduled downtime.

(c) (1) The FBI NICS Operations Center, upon receiving an FFL telephone or electronic dial-up request for a background check, will:

(i) Verify the FFL Number and code word;

(ii) Assign a NICS Transaction Number (NTN) to a valid inquiry and provide the NTN to the FFL;

(iii) Search the relevant databases (i.e., NICS Index, NCIC, III) for any matching records; and

(iv) Provide the following NICS responses based upon the consolidated NICS search results to the FFL that requested the background check:

(A) “Proceed” response, if no disqualifying information was found in the NICS Index, NCIC, or III.

(B) “Delayed” response, if the NICS search finds a record that requires more research to determine whether the prospective transferee is disqualified from possessing a firearm by Federal or state law. A “Delayed” response to the FFL indicates that the firearm transfer should not proceed pending receipt of a follow-up “Proceed” response from the NICS or the expiration of three business days (exclusive of the day on which the query is made), whichever occurs first. (Example: An FFL requests a NICS check on a prospective firearm transferee at 9:00 a.m. on Friday and shortly thereafter receives a “Delayed” response from the NICS. If state offices in the state in which the FFL is located are closed on Saturday and Sunday and open the following Monday, Tuesday, and Wednesday, and the NICS has not yet responded with a “Proceed” or “Denied” response, the FFL may transfer the firearm at 12:01 a.m. Thursday.)
(C) “Denied” response, when at least one matching record is found in either the NICS Index, NCIC, or III that provides information demonstrating that receipt of a firearm by the prospective transferee would violate 18 U.S.C. 922 or state law. The “Denied” response will be provided to the requesting FFL by the NICS Operations Center during its regular business hours.

(2) None of the responses provided to the FFL under paragraph (c)(1) of this section will contain any of the underlying information in the records checked by the system.

(d) Access to the NICS through POCs. In states where a POC is designated to process background checks for the NICS, FFLs will contact the POC to initiate a NICS background check. Both ATF and the POC will notify FFLs in the POC's state of the means by which FFLs can contact the POC. The NICS will provide POCs with electronic access to the system virtually 24 hours each day through the NCIC communication network. Upon receiving a request for a background check from an FFL, a POC will:

(1) Verify the eligibility of the FFL either by verification of the FFL number or an alternative POC-verification system;

(2) Enter a purpose code indicating that the query of the system is for the purpose of performing a NICS background check in connection with the transfer of a firearm; and (3) Transmit the request for a background check via the NCIC interface to the NICS.

(e) Upon receiving a request for a NICS background check, POCs may also conduct a search of available files in state and local law enforcement and other relevant record systems, and may provide a unique State-Assigned Transaction Number (STN) to a valid inquiry for a background check.

(f) When the NICS receives an inquiry from a POC, it will search the relevant databases (i.e., NICS Index, NCIC, III) for any matching record(s) and will provide an electronic response to the POC. This response will consolidate the search results of the relevant databases and will include the NTN. The following types of responses may be provided by the NICS to a state or local agency conducting a background check:

(1) No record response, if the NICS determines, through a complete search, that no matching record exists.

(2) Partial response, if the NICS has not completed the search of all of its records. This response will indicate the databases that have been searched (i.e.,
III, NCIC, and/or NICS Index) and the databases that have not been searched. It will also provide any potentially disqualifying information found in any of the databases searched. A follow-up response will be sent as soon as all the relevant databases have been searched. The follow-up response will provide the complete search results.

(3) Single matching record response, if all records in the relevant databases have been searched and one matching record was found.

(4) Multiple matching record response, if all records in the relevant databases have been searched and more than one matching record was found.

(g) Generally, based on the response(s) provided by the NICS, and other information available in the state and local record systems, a POC will:

(1) Confirm any matching records; and

(2) Notify the FFL that the transfer may proceed, is delayed pending further record analysis, or is denied. “Proceed” notifications made within three business days will be accompanied by the NTN or STN traceable to the NTN. The POC may or may not provide a transaction number (NTN or STN) when notifying the FFL of a “Denied” response.

(h) POC Determination Messages.
POCs shall transmit electronic NICS transaction determination messages to the FBI for the following transactions: open transactions that are not resolved before the end of the operational day on which the check is requested; denied transactions; transactions reported to the NICS as open and later changed to proceed; and denied transactions that have been overturned. The FBI shall provide POCs with an electronic capability to transmit this information. These electronic messages shall be provided to the NICS immediately upon communicating the POC determination to the FFL. For transactions where a determination has not been communicated to the FFL, the electronic messages shall be communicated no later than the end of the operational day on which the check was initiated. With the exception of permit checks, newly created POC NICS transactions that are not followed by a determination message (deny or open) before the end of the operational day on which they were initiated will be assumed to have resulted in a proceed notification to the FFL. The information provided in the POC determination messages will be maintained in the NICS Audit Log described in § 25.9(b). The NICS will destroy its records regarding POC determinations in accordance with the procedures detailed in § 25.9(b).

(i) Response recording.
FFLs are required to record the system response, whether provided by the FBI NICS Operations Center or a POC, on the appropriate ATF form for audit and
inspections purposes, under 27 CFR part 178 recordkeeping requirements. The FBI NICS Operations Center response will always include an NTN and associated “Proceed,” “Delayed,” or “Denied” determination. POC responses may vary as discussed in paragraph (g) of this section. In these instances, FFLs will record the POC response, including any transaction number and/or determination.

(j) Access to the NICS Index for purposes unrelated to NICS background checks required by the Brady Act. Access to the NICS Index for purposes unrelated to NICS background checks pursuant to 18 U.S.C. 922(t) shall be limited to uses for the purpose of:

(1) Providing information to Federal, state, or local criminal justice agencies in connection with the issuance of a firearm-related or explosives-related permit or license, including permits or licenses to possess, acquire, or transfer a firearm, or to carry a concealed firearm, or to import, manufacture, deal in, or purchase explosives; or

(2) Responding to an inquiry from the ATF in connection with a civil or criminal law enforcement activity relating to the Gun Control Act (18 U.S.C. Chapter 44) or the National Firearms Act (26 U.S.C. Chapter 53).

Official Citation:

28 CFR Section 25.7: Querying records in the system.

(a) The following search descriptors will be required in all queries of the system for purposes of a background check:

(1) Name;
(2) Sex;
(3) Race;
(4) Complete date of birth; and
(5) State of residence.

(b) A unique numeric identifier may also be provided to search for additional records based on exact matches by the numeric identifier. Examples of unique

Page 587
numeric identifiers for purposes of this system are: Social Security number (to comply with Privacy Act requirements, a Social Security number will not be required by the NICS to perform any background check) and miscellaneous identifying numbers (e.g., military number or number assigned by Federal, state, or local authorities to an individual's record). Additional identifiers that may be requested by the system after an initial query include height, weight, eye and hair color, and place of birth. At the option of the querying agency, these additional identifiers may also be included in the initial query of the system.

28 CFR Section 25.8: System safeguards.

(a) Information maintained in the NICS Index is stored electronically for use in an FBI computer environment. The NICS central computer will reside inside a locked room within a secure facility. Access to the facility will be restricted to authorized personnel who have identified themselves and their need for access to a system security officer.

(b) Access to data stored in the NICS is restricted to duly authorized agencies. The security measures listed in paragraphs (c) through (f) of this section are the minimum to be adopted by all POCs and data sources having access to the NICS.

(c) State or local law enforcement agency computer centers designated by a Control Terminal Agency as POCs shall be authorized NCIC users and shall observe all procedures set forth in the NCIC Security Policy of 1992 when processing NICS background checks. The responsibilities of the Control Terminal Agencies and the computer centers include the following:

(1) The criminal justice agency computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

(2) Since personnel at these computer centers can have access to data stored in the NICS, they must be screened thoroughly under the authority and supervision of a state Control Terminal Agency. This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a state Control Terminal Agency. This screening will also apply to non-criminal justice maintenance or technical personnel.

(3) All visitors to these computer centers must be accompanied by staff personnel at all times.
(4) POCs utilizing a state/NCIC terminal to access the NICS must have the proper computer instructions written and other built-in controls to prevent data from being accessible to any terminals other than authorized terminals.

(5) Each state Control Terminal Agency shall build its data system around a central computer, through which each inquiry must pass for screening and verification.

(d) Authorized state agency remote terminal devices operated by POCs and having access to the NICS must meet the following requirements:

(1) POCs and data sources having terminals with access to the NICS must physically place these terminals in secure locations within the authorized agency;

(2) The agencies having terminals with access to the NICS must screen terminal operators and must restrict access to the terminals to a minimum number of authorized employees; and

(3) Copies of NICS data obtained from terminal devices must be afforded appropriate security to prevent any unauthorized access or use.

(e) FFL remote terminal devices may be used to transmit queries to the NICS via electronic dial-up access. The following procedures will apply to such queries:

(1) The NICS will incorporate a security authentication mechanism that performs FFL dial-up user authentication before network access takes place;

(2) The proper use of dial-up circuits by FFLs will be included as part of the periodic audits by the FBI; and

(3) All failed authentications will be logged by the NICS and provided to the NICS security administrator.

(f) FFLs may use the telephone to transmit queries to the NICS, in accordance with the following procedures:

(1) FFLs may contact the NICS Operations Center during its regular business hours by a telephone number provided by the FBI;

(2) FFLs will provide the NICS Representative with their FFL Number and code word, the type of sale, and the name, sex, race, date of birth, and state of residence of the prospective buyer; and

(3) The NICS will verify the FFL Number and code word before processing the request.

Page 589
(g) The following precautions will be taken to help ensure the security and privacy of NICS information when FFLs contact the NICS Operations Center:

(1) Access will be restricted to the initiation of a NICS background check in connection with the proposed transfer of a firearm.

(2) The NICS Representative will only provide a response of “Proceed” or “Delayed” (with regard to the prospective firearms transfer), and will not provide the details of any record information about the transferee. In cases where potentially disqualifying information is found in response to an FFL query, the NICS Representative will provide a “Delayed” response to the FFL. Follow-up “Proceed” or “Denied” responses will be provided by the NICS Operations Center during its regular business hours.

(3) The FBI will periodically monitor telephone inquiries to ensure proper use of the system.

(h) All transactions and messages sent and received through electronic access by POCs and FFLs will be automatically logged in the NICS Audit Log described in §25.9(b). Information in the NICS Audit Log will include initiation and termination messages, failed authentications, and matching records located by each search transaction.

(i) The FBI will monitor and enforce compliance by NICS users with the applicable system security requirements outlined in the NICS POC Guidelines and the NICS FFL Manual (available from the NICS Operations Center, Federal Bureau of Investigation, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306-0147).

28 CFR Section 25.9: Retention and destruction of records in the system.

(a) The NICS will retain NICS Index records that indicate that receipt of a firearm by the individuals to whom the records pertain would violate Federal or state law. The NICS will retain such records indefinitely, unless they are canceled by the originating agency. In cases where a firearms disability is not permanent, e.g., a disqualifying restraining order, the NICS will automatically purge the pertinent record when it is no longer disqualifying. Unless otherwise removed, records contained in the NCIC and III files that are accessed during a background check will remain in those files in accordance with established policy.

(b) The FBI will maintain an automated NICS Audit Log of all incoming and outgoing transactions that pass through the system.
(1) Contents.

The NICS Audit Log will record the following information: Type of transaction (inquiry or response), line number, time, date of inquiry, header, message key, ORI or FFL identifier, and inquiry/response data (including the name and other identifying information about the prospective transferee and the NTN).

(i) NICS Audit Log records relating to denied transactions will be retained for 10 years, after which time they will be transferred to a Federal Records Center for storage;

(ii) NICS Audit Log records relating to transactions in an open status, except the NTN and date, will be destroyed after not more than 90 days from the date of inquiry; and

(iii) In cases of NICS Audit Log records relating to allowed transactions, all identifying information submitted by or on behalf of the transferee will be destroyed within 24 hours after the FFL receives communication of the determination that the transfer may proceed. All other information, except the NTN and date, will be destroyed after not more than 90 days from the date of inquiry.

(2) Use of information in the NICS Audit Log.

The NICS Audit Log will be used to analyze system performance, assist users in resolving operational problems, support the appeals process, or support audits of the use and performance of the system. Searches may be conducted on the Audit Log by time frame, i.e., by day or month, or by a particular state or agency. Information in the NICS Audit Log pertaining to allowed transactions may be accessed directly only by the FBI and only for the purpose of conducting audits of the use and performance of the NICS, except that:

(i) Information in the NICS Audit Log, including information not yet destroyed under § 5.9(b)(1)(iii), that indicates, either on its face or in conjunction with other information, a violation or potential violation of law or regulation, may be shared with appropriate authorities responsible for investigating, prosecuting, and/or enforcing such law or regulation; and

(ii) The NTNs and dates for allowed transactions may be shared with ATF in Individual FFL Audit Logs as specified in § 25.9(b)(4).

(3) Limitation on use.
The NICS, including the NICS Audit Log, may not be used by any Department, agency, officer, or employee of the United States to establish any system for the registration of firearms, firearm owners, or firearm transactions or dispositions, except with respect to persons prohibited from receiving a firearm by 18 U.S.C. 922(g) or (n) or by state law. The NICS Audit Log will be monitored and reviewed on a regular basis to detect any possible misuse of NICS data.

(4) Creation and Use of Individual FFL Audit Logs.

Upon written request from ATF containing the name and license number of the FFL and the proposed date of inspection of the named FFL by ATF, the FBI may extract information from the NICS Audit Log and create an Individual FFL Audit Log for transactions originating at the named FFL for a limited period of time. An Individual FFL Audit Log shall contain all information on denied transactions, and, with respect to all other transactions, only non-identifying information from the transaction. In no instance shall an Individual FFL Audit Log contain more than 60 days worth of allowed or open transaction records originating at the FFL. The FBI will provide POC states the means to provide to the FBI information that will allow the FBI to generate Individual FFL Audit Logs in connection with ATF inspections of FFLs in POC states. POC states that elect not to have the FBI generate Individual FFL Audit Logs for FFLs in their states must develop a means by which the POC will provide such Logs to ATF.

(c) The following records in the FBI-operated terminals of the NICS will be subject to the Brady Act’s requirements for destruction:

(1) All inquiry and response messages (regardless of media) relating to a background check that results in an allowed transfer; and

(2) All information (regardless of media) contained in the NICS Audit Log relating to a background check that results in an allowed transfer.

(d) The following records of state and local law enforcement units serving as POCs will be subject to the Brady Act’s requirements for destruction:

(1) All inquiry and response messages (regardless of media) relating to the initiation and result of a check of the NICS that allows a transfer that are not part of a record system created and maintained pursuant to independent state law regarding firearms transactions; and

(2) All other records relating to the person or the transfer created as a result of a NICS check that are not part of a record system created and maintained pursuant to independent state law regarding firearms transactions.

Official Citation:
28 CFR Section 25.10: Correction of erroneous system information.

(a) An individual may request the reason for the denial from the agency that conducted the check of the NICS (the “denying agency,” which will be either the FBI or the state or local law enforcement agency serving as a POC). The FFL will provide to the denied individual the name and address of the denying agency and the unique transaction number (NTN or STN) associated with the NICS background check. The request for the reason for the denial must be made in writing to the denying agency. (POCs at their discretion may waive the requirement for a written request.)

(b) The denying agency will respond to the individual with the reasons for the denial within five business days of its receipt of the individual's request. The response should indicate whether additional information or documents are required to support an appeal, such as fingerprints in appeals involving questions of identity (i.e., a claim that the record in question does not pertain to the individual who was denied).

(c) If the individual wishes to challenge the accuracy of the record upon which the denial is based, or if the individual wishes to assert that his or her rights to possess a firearm have been restored, he or she may make application first to the denying agency, i.e., either the FBI or the POC. If the denying agency is unable to resolve the appeal, the denying agency will so notify the individual and shall provide the name and address of the agency that originated the document containing the information upon which the denial was based. The individual may then apply for correction of the record directly to the agency from which it originated. If the record is corrected as a result of the appeal to the originating agency, the individual may so notify the denying agency, which will, in turn, verify the record correction with the originating agency (assuming the originating agency has not already notified the denying agency of the correction) and take all necessary steps to correct the record in the NICS.

(d) As an alternative to the above procedure where a POC was the denying agency, the individual may elect to direct his or her challenge to the accuracy of the record, in writing, to the FBI, NICS Operations Center, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Module C-3, Clarksburg, West Virginia 26306-0147. Upon receipt of the information, the FBI will investigate the matter by contacting the POC that denied the transaction or the data source. The FBI will request the POC or the data source to verify that the
record in question pertains to the individual who was denied, or to verify or correct the challenged record. The FBI will consider the information it receives from the individual and the response it receives from the POC or the data source. If the record is corrected as a result of the challenge, the FBI shall so notify the individual, correct the erroneous information in the NICS, and give notice of the error to any Federal department or agency or any state that was the source of such erroneous records.

(e) Upon receipt of notice of the correction of a contested record from the originating agency, the FBI or the agency that contributed the record shall correct the data in the NICS and the denying agency shall provide a written confirmation of the correction of the erroneous data to the individual for presentation to the FFL. If the appeal of a contested record is successful and thirty (30) days or less have transpired since the initial check, and there are no other disqualifying records upon which the denial was based, the NICS will communicate a “Proceed” response to the FFL. If the appeal is successful and more than thirty (30) days have transpired since the initial check, the FFL must recheck the NICS before allowing the sale to continue. In cases where multiple disqualifying records are the basis for the denial, the individual must pursue a correction for each record.

(f) An individual may also contest the accuracy or validity of a disqualifying record by bringing an action against the state or political subdivision responsible for providing the contested information, or responsible for denying the transfer, or against the United States, as the case may be, for an order directing that the contested information be corrected or that the firearm transfer be approved.

(g) An individual may provide written consent to the FBI to maintain information about himself or herself in a Voluntary Appeal File to be established by the FBI and checked by the NICS for the purpose of preventing the future erroneous denial or extended delay by the NICS of a firearm transfer. Such file shall be used only by the NICS for this purpose. The FBI shall remove all information in the Voluntary Appeal File pertaining to an individual upon receipt of a written request by that individual. However, the FBI may retain such information contained in the Voluntary Appeal File as long as needed to pursue cases of identified misuse of the system. If the FBI finds a disqualifying record on the individual after his or her entry into the Voluntary Appeal File, the FBI may remove the individual's information from the file.

Official Citation:
(a) State or local agencies, FFLs, or individuals violating this subpart A shall be subject to a fine not to exceed $10,000 and subject to cancellation of NICS inquiry privileges.

(b) Misuse or unauthorized access includes, but is not limited to, the following:

   (1) State or local agencies', FFLs', or individuals' purposefully furnishing incorrect information to the system to obtain a “Proceed” response, thereby allowing a firearm transfer;

   (2) State or local agencies', FFLs', or individuals' purposefully using the system to perform a check for unauthorized purposes; and

   (3) Any unauthorized person's accessing the NICS.
28 CFR Section 25.51: Purpose and authority.

The purpose of this subpart is to establish policies and procedures implementing the National Motor Vehicle Title Information System (NMVTIS) in accordance with title 49 U.S.C. 30502. The purpose of NMVTIS is to assist in efforts to prevent the introduction or reintroduction of stolen motor vehicles into interstate commerce, protect states and individual and commercial consumers from fraud, reduce the use of stolen vehicles for illicit purposes including fundraising for criminal enterprises, and provide consumer protection from unsafe vehicles.

28 CFR Section 25.52: Definitions.

For purposes of this subpart B:

Acquiring
means owning, possessing, handling, directing, or controlling.

Automobile
has the same meaning given that term in 49 U.S.C. 32901(a).

Certificate of title
means a document issued by a state showing ownership of an automobile.

Insurance carrier
means an individual or entity engaged in the business of underwriting automobile insurance.

Junk automobile
means an automobile that—

(1) Is incapable of operating on public streets, roads, and highways; and
(2) Has no value except as a source of parts or scrap.

Junk yard means an individual or entity engaged in the business of acquiring or owning junk automobiles for—

(1) Resale in their entirety or as spare parts; or

(2) Rebuilding, restoration, or crushing.

Motor vehicle
has the same meaning given that term in 49 U.S.C. 3102(6).

NMVTIS
means the National Motor Vehicle Title Information System.

Operator
means the individual or entity authorized or designated as the operator of NMVTIS under 49 U.S.C. 30502(b), or the office designated by the Attorney General, if there is no authorized or designated individual or entity.

Purchaser
means the individual or entity buying an automobile or financing the purchase of an automobile. For purposes of this subpart, purchasers include dealers, auction companies or entities engaged in the business of purchasing used automobiles, lenders financing the purchase of new or used automobiles, and automobile dealers.

Salvage automobile
means an automobile that is damaged by collision, fire, flood, accident, trespass, or other event, to the extent that its fair salvage value plus the cost of repairing the automobile for legal operation on public streets, roads, and highways would be more than the fair market value of the automobile immediately before the event that caused the damage. Salvage automobiles include automobiles determined to be a total loss under the law of the applicable jurisdiction or designated as a total loss by an insurer under the terms of its policies, regardless of whether or not the ownership of the vehicle is transferred to the insurance carrier.
Salvage yard means an individual or entity engaged in the business of acquiring or owning salvage automobiles for—

(1) Resale in their entirety or as spare parts; or

(2) Rebuilding, restoration, or crushing.

Note to definition of “Salvage yard”: For purposes of this subpart, vehicle remarketers and vehicle recyclers, including scrap vehicle shredders and scrap metal processors as well as “pull- or pick-apart yards,” salvage pools, salvage auctions, and other types of auctions handling salvage or junk vehicles (including vehicles declared a “total loss”), are included in the definition of “junk or salvage yards.”

State means a state of the United States or the District of Columbia.

Total loss means that the cost of repairing such vehicles plus projected supplements plus projected diminished resale value plus rental reimbursement expense exceeds the cost of buying the damaged motor vehicle at its pre-accident value, minus the proceeds of selling the damaged motor vehicle for salvage.

VIN means the vehicle identification number;

28 CFR Section 25.53: Responsibilities of the operator of NMVTIS.

(a) By no later than March 31, 2009, the operator shall make available:

(1) To a participating state on request of that state, information in NMVTIS about any automobile;

(2) To a Government, state, or local law enforcement official on request of that official, information in NMVTIS about a particular automobile, junk yard, or salvage yard;

(3) To a prospective purchaser of an automobile on request of that purchaser, information in NMVTIS about that automobile; and
(4) To a prospective or current insurer of an automobile on request of that insurer, information in NMVTIS about the automobile.

(b) NMVTIS shall permit a user of the system to establish instantly and reliably:

(1) The validity and status of a document purporting to be a certificate of title;

(2) Whether an automobile bearing a known VIN is titled in a particular state;

(3) Whether an automobile known to be titled in a particular state is or has been a junk automobile or a salvage automobile;

(4) For an automobile known to be titled in a particular state, the odometer mileage disclosure required under 49 U.S.C. 32705 for that automobile on the date the certificate of title for that automobile was issued and any later mileage information, if noted by the state; and

(5) Whether an automobile bearing a known VIN has been reported as a junk automobile or a salvage automobile under 49 U.S.C. 30504.

(c) The operator is authorized to seek and accept, with the concurrence of the Department of Justice, additional information from states and public and private entities that is relevant to the titling of automobiles and to assist in efforts to prevent the introduction or reintroduction of stolen motor vehicles and parts into interstate commerce. The operator, however, may not collect any social security account numbers as part of any of the information provided by any state or public or private entity. The operator may not make personally identifying information contained within NMVTIS, such as the name or address of the owner of an automobile, available to an individual prospective purchaser. With the approval of the Department of Justice, the operator may allow public and private entities that provide information to NMVTIS to query the system if such access will assist in efforts to prevent the introduction or reintroduction of stolen motor vehicles and parts into interstate commerce.

(d) The operator shall develop and maintain a privacy policy that addresses the information in the system and how personal information shall be protected. DOJ shall review and approve this privacy policy.

(e) The means by which access is provided by the operator to users of NMVTIS must be approved by the Department of Justice.
(f) The operator shall biennially establish and at least annually collect user fees from the states and users of NMVTIS to pay for its operation, but the operator may not collect fees in excess of the costs of operating the system. The operator is required to recalculate the user fees on a biennial basis. After the operator establishes its initial user fees for the states under this section, subsequent state user fees must be established at least one year in advance of their effective date. Any user fees established by the operator must be established with the approval of the Department of Justice. The operator of NMVTIS will inform the states of the applicable user fees either through publication in the Federal Register or by direct notice or invoice to the states.

(1) The expenses to be recouped by the operator of NMVTIS will consist of labor costs, data center operations costs, the cost of providing access to authorized users, annual functional enhancement costs (including labor and hardware), costs necessary for implementing the provisions of this rule, the cost of technical upgrades, and other costs approved in advance by the Department of Justice.

(2) User fees collected from states should be based on the states' pro rata share of the total number of titled motor vehicles based on the Highway Statistics Program of the Federal Highway Administration, U.S. Department of Transportation, except in cases where states did not report to that program, in which case the states shall make available the most recent statistics for motor vehicle title registrations.

(3) All states, regardless of their level of participation, shall be charged user fees by the operator.

(4) No fees shall be charged for inquiries from law enforcement agencies.

(g) The operator will establish procedures and practices to facilitate reporting to NMVTIS in the least burdensome and costly fashion. If the operator is not the Department of Justice, the operator must provide an annual report to the Department of Justice detailing the fees it collected and how it expended such fees and other funds to operate NMVTIS. This report must also include a status report on the implementation of the system, compliance with reporting and other requirements, and sufficient detail and scope regarding financial information so that reasonable determinations can be made regarding budgeting and performance. The operator shall procure an independent financial audit of NMVTIS revenues and expenses on an annual basis. The Department of Justice will make these reports available for public inspection.

28 CFR Section 25.54: Responsibilities of the States.
(a) Each state must maintain at least the level of participation in NMVTIS that it had achieved as of January 1, 2009. By no later than January 1, 2010, each state must have completed implementation of all requirements of participation and provide, or cause to be provided by an agent or third party, to the designated operator and in an electronic format acceptable to the operator, at a frequency of once every 24 hours, titling information for all automobiles maintained by the state. The titling information provided to NMVTIS must include the following:

(1) VIN;

(2) Any description of the automobile included on the certificate of title (including any and all brands associated with such vehicle);

(3) The name of the individual or entity to whom the certificate was issued;

(4) Information from junk or salvage yard operators or insurance carriers regarding the acquisition of junk automobiles or salvage automobiles, if this information is being collected by the state; and

(5) For an automobile known to be titled in a particular state, the odometer mileage disclosure required under 49 U.S.C. 32705 for that automobile on the date the certificate of title for that automobile was issued and any later mileage information, if noted by the state.

(b) With the approval of the operator and the state, the titling information provided to NMVTIS may include any other information included on the certificates of title and any other information the state maintains in relation to these titles.

(c) By no later than January 1, 2010, each state shall establish a practice of performing a title verification check through NMVTIS before issuing a certificate of title to an individual or entity claiming to have purchased an automobile from an individual or entity in another state or in cases of title transfers. The check will consist of—

(1) Communicating to the operator the VIN of the automobile for which the certificate of title is sought;

(2) Giving the operator an opportunity to communicate to the participating state the results of a search of the information and using the results to determine the validity and status of a document purporting to be a certification of title, to determine whether the automobile has been a junk or salvage vehicle or has been reported as such, to compare and verify the odometer information
presented with that reported in the system, and to determine the validity of other information presented (e.g., lien-holder status, etc.).

(d) By January 1, 2010, those states not currently paying user fees will be responsible for paying user fees as established by the operator to support NMVTIS.

28 CFR Section 25.55: Responsibilities of insurance carriers.

(a) By no later than March 31, 2009, and on a monthly basis as designated by the operator, any individual or entity acting as an insurance carrier conducting business within the United States shall provide, or cause to be provided on its behalf, to the operator and in a format acceptable to the operator, a report that contains an inventory of all automobiles of the current model year or any of the four prior model years that the carrier, during the past month, has obtained possession of and has decided are junk automobiles or salvage automobiles. An insurance carrier shall report on any automobiles that it has determined to be a total loss under the law of the applicable jurisdiction (i.e., state) or designated as a total loss by the insurance company under the terms of its policies.

(b) The inventory must contain the following information:

(1) The name, address, and contact information for the reporting entity (insurance carrier);

(2) VIN;

(3) The date on which the automobile was obtained or designated as a junk or salvage automobile;

(4) The name of the individual or entity from whom the automobile was obtained and who possessed it when the automobile was designated as a junk or salvage automobile; and

(5) The name of the owner of the automobile at the time of the filing of the report.

(c) Insurance carriers are strongly encouraged to provide the operator with information on other motor vehicles or other information relevant to a motor vehicle’s title, including the reason why the insurance carrier obtained possession of the motor vehicle. For example, the insurance carrier may have obtained possession of a motor vehicle because it had been subject to flood, water, collision, or fire damage, or as a result of theft and recovery. The provision of
information provided by an insurance carrier under this paragraph must be pursuant to a means approved by the operator.

(d) Insurance carriers whose required data is provided to the operator through an operator-authorized third party in a manner acceptable to the operator are not required to duplicate such reporting. For example, if the operator and a private third-party organization reach agreement on the provision of insurance data already reported by insurance to the third party, insurance companies are not required to subsequently report the information directly into NMVTIS.

28 CFR Section 25.56: Responsibilities of junk yards and salvage yards and auto recyclers.

(a) By no later than March 31, 2009, and continuing on a monthly basis as designated by the operator, any individual or entity engaged in the business of operating a junk yard or salvage yard within the United States shall provide, or cause to be provided on its behalf, to the operator and in a format acceptable to the operator, an inventory of all junk automobiles or salvage automobiles obtained in whole or in part by that entity in the prior month.

(b) The inventory shall include the following information:

(1) The name, address, and contact information for the reporting entity (junk, salvage yard, recycler);

(2) VIN;

(3) The date the automobile was obtained;

(4) The name of the individual or entity from whom the automobile was obtained;

(5) A statement of whether the automobile was crushed or disposed of, for sale or other purposes, to whom it was provided or transferred, and if the vehicle is intended for export out of the United States.

(c) Junk and salvage yards, however, are not required to report this information if they already report the information to the state and the state makes the information required in this rule available to the operator.

(d) Junk and salvage yards may be required to file an update or supplemental report of final disposition of any automobile where final disposition information
was not available at the time of the initial report filing, or if their actual disposition of the automobile differs from what was initially reported.

(e) Junk and salvage yards are encouraged to provide the operator with similar information on motor vehicles other than automobiles that they obtain that possess VINs.

(f) Junk- and salvage-yard operators whose required data is provided to the operator through an operator-authorized third party (e.g., state or other public or private organization) in a manner acceptable to the operator are not required to duplicate such reporting. In addition, junk and salvage yards are not required to report on an automobile if they are issued a verification under 49 U.S.C. 33110 stating that the automobile or parts from the automobile are not reported as stolen.

(g) Such entities must report all salvage or junk vehicles they obtain, including vehicles from or on behalf of insurance carriers, which can be reasonably assumed are total loss vehicles. Such entities, however, are not required to report any vehicle that is determined not to meet the definition of salvage or junk after a good-faith physical and value appraisal conducted by qualified appraisal personnel, so long as such appraisals are conducted entirely independent of any other interests, persons or entities. Individuals and entities that handle less than five vehicles per year that are determined to be salvage, junk, or total loss are not required to report under the salvage-yard requirements.

(h) Scrap metal processors and shredders that receive automobiles for recycling where the condition of such vehicles generally prevent VINs from being identified are not required to report to the operator if the source of each vehicle has already reported the vehicle to NMVTIS. In cases where a supplier's compliance with NMVTIS cannot be ascertained, however, scrap metal processors and shredders must report these vehicles to the operator based on a visual inspection if possible. If the VIN cannot be determined based on this inspection, scrap metal processors and shredders may rely on primary documentation (i.e., title documents) provided by the vehicle supplier.

28 CFR Section 25.57: Erroneous junk or salvage reporting.

(a) In cases where a vehicle is erroneously reported to have been salvage or junk and subsequently destroyed (i.e., crushed), owners of the legitimate vehicles are encouraged to seek a vehicle inspection in the current state of title whereby inspection officials can verify via hidden VINs the vehicle's true identity. Owners
are encouraged to file such inspection reports with the current state of title and to retain such reports so that the vehicle's true history can be documented.

(b) To avoid the possibility of fraud, the operator may not allow any entity to delete a prior report of junk or salvage status.
28 CFR PART 27—WHISTLEBLOWER PROTECTION FOR FEDERAL BUREAU OF INVESTIGATION EMPLOYEES

- Subpart A—Protected Disclosures of Information
  - 28 CFR Section 27.1: Making a protected disclosure.
  - 28 CFR Section 27.2: Prohibition against reprisal for making a protected disclosure.

- Subpart B—Investigating Reprisal Allegations and Ordering Corrective Action
  - 28 CFR Section 27.4: Corrective action and other relief; Director, Office of Attorney Recruitment and Management.
  - 28 CFR Section 27.5: Review.
  - 28 CFR Section 27.6: Extensions of time.

Authority:

Source:
Order No. 2264-99, 64 FR 58786, Nov. 1, 1999, unless otherwise noted.
SUBPART A—Protected Disclosures of Information

28 CFR Section 27.1: Making a protected disclosure.

(a) When an employee of, or applicant for employment with, the Federal Bureau of Investigation (FBI) (FBI employee) makes a disclosure of information to the Department of Justice's (Department's) Office of Professional Responsibility (OPR), the Department's Office of Inspector General (OIG), the FBI Office of Professional Responsibility (FBI OPR), the FBI Inspection Division (FBI-INSD) Internal Investigations Section (collectively, Receiving Offices), the Attorney General, the Deputy Attorney General, the Director of the FBI, the Deputy Director of the FBI, or to the highest ranking official in any FBI field office, the disclosure will be a “protected disclosure” if the person making it reasonably believes that it evidences:

   (1) A violation of any law, rule or regulation; or

   (2) Mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(b) Any office or official (other than the OIG or OPR) receiving a protected disclosure shall promptly report such disclosure to the OIG or OPR for investigation. The OIG and OPR shall proceed in accordance with procedures establishing their respective jurisdiction. The OIG or OPR may refer such allegations to FBI-INSD Internal Investigations Section for investigation unless the Deputy Attorney General determines that such referral shall not be made. 

Official Citation:
[Order No. 2926-2008, 73 FR 1495, Jan. 9, 2008]

28 CFR Section 27.2: Prohibition against reprisal for making a protected disclosure.

(a) Any employee of the FBI, or of any other component of the Department, who has authority to take, direct others to take, recommend, or approve any personnel action shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a personnel action, as defined below, with respect to any FBI employee as a reprisal for a protected disclosure.

(b) Personnel action means any action described in clauses (i) through (xi) of 5 U.S.C. 2302(a)(2)(A) taken with respect to an FBI employee other than one in a position which the Attorney General has designated in advance of encumbrance as being a position of a confidential, policy-determining, policy-making, or policy-advocating character.

Page 607

(a)(1) An FBI employee who believes that another employee of the FBI, or of any other Departmental component, has taken or has failed to take a personnel action as a reprisal for a protected disclosure (reprisal), may report the alleged reprisal to either the Department's OPR or the Department's OIG (collectively, Investigative Offices). The report of an alleged reprisal must be made in writing.

(2) For purposes of this subpart, references to the FBI include any other Departmental component in which the person or persons accused of the reprisal were employed at the time of the alleged reprisal.

(b) The Investigative Office that receives the report of an alleged reprisal shall consult with the other Investigative Office to determine which office is more suited, under the circumstances, to conduct an investigation into the allegation. The Attorney General retains final authority to designate or redesignate the Investigative Office that will conduct an investigation.

(c) Within 15 calendar days of the date the allegation of reprisal is first received by an Investigative Office, the office that will conduct the investigation (Conducting Office) shall provide written notice to the person who made the allegation (Complainant) indicating—

(1) That the allegation has been received; and

(2) The name of a person within the Conducting Office who will serve as a contact with the Complainant.

(d) The Conducting Office shall investigate any allegation of reprisal to the extent necessary to determine whether there are reasonable grounds to believe that a reprisal has been or will be taken.

(e) Within 90 calendar days of providing the notice required in paragraph (c) of this section, and at least every 60 calendar days thereafter (or at any other time if the Conducting Office deems appropriate), the Conducting Office shall notify the Complainant of the status of the investigation.

(f) The Conducting Office shall determine whether there are reasonable grounds to believe that there has been or will be a reprisal for a protected disclosure. The Conducting Office shall make this determination within 240 calendar days of receiving the allegation of reprisal unless the Complainant agrees to an extension.
(g) If the Conducting Office decides to terminate an investigation, it shall provide, no later than 10 business days before providing the written statement required by paragraph (h) of this section, a written status report to the Complainant containing the factual findings and conclusions justifying the termination of the investigation. The Complainant may submit written comments on such report to the Conducting Office. The Conducting Office shall not be required to provide a subsequent written status report after submission of such comments.

(h) If the Conducting Office terminates an investigation, it shall prepare and transmit to the Complainant a written statement notifying him/her of—

   (1) The termination of the investigation;

   (2) A summary of relevant facts ascertained by the Conducting Office;

   (3) The reasons for termination of the investigation; and

   (4) A response to any comments submitted under paragraph (g) of this section.

   (i) Such written statement prepared pursuant to paragraph (h) of this section may not be admissible as evidence in any subsequent proceeding without the consent of the Complainant.

(j) Nothing in this part shall prohibit the Receiving Offices, in the absence of a reprisal allegation by an FBI employee under this part, from conducting an investigation, under their pre-existing jurisdiction, to determine whether a reprisal has been or will be taken.

28 CFR Section 27.4: Corrective action and other relief; Director, Office of Attorney Recruitment and Management.

(a) If, in connection with any investigation, the Conducting Office determines that there are reasonable grounds to believe that a reprisal has been or will be taken, the Conducting Office shall report this conclusion, together with any findings and recommendations for corrective action, to the Director, Office of Attorney Recruitment and Management (the Director). If the Conducting Office's report to the Director includes a recommendation for corrective action, the Director shall provide an opportunity for comments on the report by the FBI and the Complainant. The Director, upon receipt of the Conducting Office's report, shall proceed in accordance with paragraph (e) of this section. A determination by the Conducting Office that there are reasonable grounds to believe a reprisal
has been or will be taken shall not be cited or referred to in any proceeding under these regulations, without the Complainant’s consent.

(b) At any time, the Conducting Office may request the Director to order a stay of any personnel action for 45 calendar days if it determines that there are reasonable grounds to believe that a reprisal has been or is to be taken. The Director shall order such stay within three business days of receiving the request for stay, unless the Director determines that, under the facts and circumstances involved, such a stay would not be appropriate. The Director may extend the period of any stay granted under this paragraph for any period that the Director considers appropriate. The Director shall allow the FBI an opportunity to comment to the Director on any proposed extension of a stay, and may request additional information as the Director deems necessary. The Director may terminate a stay at any time, except that no such termination shall occur until the Complainant and the Conducting Office shall first have had notice and an opportunity to comment.

(c)(1) The Complainant may present a request for corrective action directly to the Director within 60 calendar days of receipt of notification of termination of an investigation by the Conducting Office or at any time after 120 calendar days from the date the Complainant first notified an Investigative Office of an alleged reprisal if the Complainant has not been notified by the Conducting Office that it will seek corrective action. The Director shall notify the FBI of the receipt of the request and allow the FBI 25 calendar days to respond in writing. If the Complainant presents a request for corrective action to the Director under this paragraph, the Conducting Office may continue to seek corrective action specific to the Complainant, including the submission of a report to the Director, only with the Complainant’s consent. Notwithstanding the Complainant’s refusal of such consent, the Conducting Office may continue to investigate any violation of law, rule, or regulation.

(2) The Director may not direct the Conducting Office to reinstate an investigation that the Conducting Office has terminated in accordance with § 27.3(h).

(d) Where a Complainant has presented a request for corrective action to the Director under paragraph (c) of this section, the Complainant may at any time request the Director to order a stay of any personnel action allegedly taken or to be taken in reprisal for a protected disclosure. The request for a stay must be in writing, and the FBI shall have an opportunity to respond. The request shall be granted within 10 business days of the receipt of any response by the FBI if the Director determines that such a stay would be appropriate. A stay granted under this paragraph shall remain in effect for such period as the Director deems appropriate. The Director may modify or dissolve a stay under this paragraph at any time if the Director determines that such a modification or dissolution is appropriate.
(e)(1) The Director shall determine, based upon all the evidence, whether a protected disclosure was a contributing factor in a personnel action taken or to be taken. Subject to paragraph (e)(2) of this section, if the Director determines that a protected disclosure was a contributing factor in a personnel action taken or to be taken, the Director shall order corrective action as the Director deems appropriate. The Director may conclude that the disclosure was a contributing factor in the personnel action based upon circumstantial evidence, such as evidence that the employee taking the personnel action knew of the disclosure and that the personnel action occurred within a period of time such that a reasonable person could conclude that the disclosure was a contributing factor in the personnel action.

(2) Corrective action may not be ordered if the FBI demonstrates by clear and convincing evidence that it would have taken the same personnel action in the absence of such disclosure.

(3) In making the determinations required under this subsection, the Director may hold a hearing at which the Complainant may present evidence in support of his or her claim, in accordance with such procedures as the Director may adopt. The Director is hereby authorized to compel the attendance and testimony of, or the production of documentary or other evidence from, any person employed by the Department if doing so appears reasonably calculated to lead to the discovery of admissible evidence, is not otherwise prohibited by law or regulation, and is not unduly burdensome. Any privilege available in judicial and administrative proceedings relating to the disclosure of documents or the giving of testimony shall be available before the Director. All assertions of such privileges shall be decided by the Director. The Director may, upon request, certify a ruling on an assertion of privilege for review by the Deputy Attorney General.

(f) If the Director orders corrective action, such corrective action may include: placing the Complainant, as nearly as possible, in the position he would have been in had the reprisal not taken place; reimbursement for attorneys fees, reasonable costs, medical costs incurred, and travel expenses; back pay and related benefits; and any other reasonable and foreseeable consequential damages.

(g) If the Director determines that there has not been a reprisal, the Director shall report this finding in writing to the complainant, the FBI, and the Conducting Office.

Official Citation:
28 CFR Section 27.5: Review.

The Complainant or the FBI may request, within 30 calendar days of a final determination or corrective action order by the Director, review by the Deputy Attorney General of that determination or order. The Deputy Attorney General shall set aside or modify the Director's actions, findings, or conclusions found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; obtained without procedures required by law, rule, or regulation having been followed; or unsupported by substantial evidence. The Deputy Attorney General has full discretion to review and modify corrective action ordered by the Director, provided, however that if the Deputy Attorney General upholds a finding that there has been a reprisal, then the Deputy Attorney General shall order appropriate corrective action.

28 CFR Section 27.6: Extensions of time.

The Director may extend, for extenuating circumstances, any of the time limits provided in these regulations relating to proceedings before him and to requests for review by the Deputy Attorney General.
28 CFR PART 28—DNA IDENTIFICATION SYSTEM

➢ Subpart A—Qualifying Federal Offenses for Purposes of DNA Sample Collection
  o 28 CFR Section 28.1: Purpose.
  o 28 CFR Section 28.2: Determination of offenses.
➢ Subpart B—DNA Sample Collection, Analysis, and Indexing
  o 28 CFR Section 28.11: Definitions.
  o 28 CFR Section 28.12: Collection of DNA samples.
➢ Subpart C—Preservation of Biological Evidence
  o 28 CFR Section 28.21: Purpose.
  o 28 CFR Section 28.22: The requirement to preserve biological evidence.
  o 28 CFR Section 28.23: Evidence subject to the preservation requirement.
  o 28 CFR Section 28.24: Exceptions based on the results of judicial proceedings.
  o 28 CFR Section 28.25: Exceptions based on a defendant’s conduct.
  o 28 CFR Section 28.26: Exceptions based on the nature of the evidence.
  o 28 CFR Section 28.27: Non-preemption of other requirements.
  o 28 CFR Section 28.28: Sanctions for violations.

Authority:

Source:
Order No. 2699-2003, 68 FR 74858, Dec. 29, 2003, unless otherwise noted.
SUBPART A—Qualifying Federal Offenses for Purposes of DNA Sample Collection

28 CFR Section 28.1: Purpose.

Section 3 of Pub. L. 106-546 directs the collection, analysis, and indexing of a DNA sample from each individual in the custody of the Bureau of Prisons or under the supervision of a probation office who is, or has been, convicted of a qualifying Federal offense. Subsection (d) of that section states that the offenses that shall be treated as qualifying Federal offenses are any felony and certain other types of offenses, as determined by the Attorney General.

Official Citation:

28 CFR Section 28.2: Determination of offenses.

(a) Felony
means a Federal offense that would be classified as a felony under 18 U.S.C. 3559(a) or that is specifically classified by a letter grade as a felony.

(b) The following offenses shall be treated for purposes of section 3 of Pub. L. 106-546 as qualifying Federal offenses:

(1) Any felony.

(2) Any offense under chapter 109A of title 18, United States Code, even if not a felony.

(3) Any offense under any of the following sections of the United States Code, even if not a felony:

   (i) In title 18, section 111, 112(b) involving intimidation or threat, 113, 115, 245, 247, 248 unless the offense involves only a nonviolent physical obstruction and is not a felony, 351, 594, 1153 involving assault against an individual who has not attained the age of 16 years, 1361, 1368, the second paragraph of 1501, 1509, 1751, 1991, or 2194 involving force or threat.

   (ii) In title 16, section 773g if the offense involves a violation of section 773e(a)(3), 1859 if the offense involves a violation of section 1857(1)(E), 3637(c) if the offense involves a violation of section 3637(a)(3), or 5010(b) if the offense involves a violation of section 5009(6).

   (iii) In title 26, section 7212.
(iv) In title 30, section 1463 if the offense involves a violation of section 1461(4).

(v) In title 40, section 5109 if the offense involves a violation or attempted violation of section 5104(e)(2)(F).

(vi) In title 42, section 2283, 3631, or 9152(d) if the offense involves a violation of section 9151(3).

(vii) In title 43, section 1063 involving force, threat, or intimidation.

(viii) In title 47, section 606(b).

(ix) In title 49, section 46506(1) unless the offense involves only an act that would violate section 661 or 662 of title 18 and would not be a felony if committed in the special maritime and territorial jurisdiction of the United States.

(4) Any offense that is an attempt or conspiracy to commit any of the foregoing offenses, even if not a felony.

(c) An offense that was or would have been a qualifying Federal offense as defined in this section at the time of conviction, such as an offense under 18 U.S.C. 2031 or 2032, remains a qualifying Federal offense even if the provision or provisions defining the offense or assigning its penalties have subsequently been repealed, superseded, or modified.

**Official Citation:**
SUBPART B—DNA Sample Collection, Analysis, and Indexing

28 CFR Section 28.11: Definitions.

DNA analysis means analysis of the deoxyribonucleic acid (DNA) identification information in a bodily sample.

DNA sample means a tissue, fluid, or other bodily sample of an individual on which a DNA analysis can be carried out.

28 CFR Section 28.12: Collection of DNA samples.

(a) The Bureau of Prisons shall collect a DNA sample from each individual in the custody of the Bureau of Prisons who is, or has been, convicted of—

   (1) A Federal offense (including any offense under the Uniform Code of Military Justice); or

   (2) A qualifying District of Columbia offense, as determined under section 4(d) of Public Law 106-546.

(b) Any agency of the United States that arrests or detains individuals or supervises individuals facing charges shall collect DNA samples from individuals who are arrested, facing charges, or convicted, and from non-United States persons who are detained under the authority of the United States. For purposes of this paragraph, “non-United States persons” means persons who are not United States citizens and who are not lawfully admitted for permanent residence as defined in 8 CFR 1.1(p). Unless otherwise directed by the Attorney General, the collection of DNA samples under this paragraph may be limited to individuals from whom the agency collects fingerprints and may be subject to other limitations or exceptions approved by the Attorney General. The DNA-sample collection requirements for the Department of Homeland Security in relation to non-arrestees do not include, except to the extent provided by the Secretary of Homeland Security, collecting DNA samples from:

   (1) Aliens lawfully in, or being processed for lawful admission to, the United States;

   (2) Aliens held at a port of entry during consideration of admissibility and not subject to further detention or proceedings;
(3) Aliens held in connection with maritime interdiction; or

(4) Other aliens with respect to whom the Secretary of Homeland Security, in consultation with the Attorney General, determines that the collection of DNA samples is not feasible because of operational exigencies or resource limitations.

(c) The DNA-sample collection requirements under this section shall be implemented by each agency by January 9, 2009.

(d) Each individual described in paragraph (a) or (b) of this section shall cooperate in the collection of a DNA sample from that individual. Agencies required to collect DNA samples under this section may use or authorize the use of such means as are reasonably necessary to detain, restrain, and collect a DNA sample from an individual described in paragraph (a) or (b) of this section who refuses to cooperate in the collection of the sample.

(e) Agencies required to collect DNA samples under this section may enter into agreements with other agencies described in paragraph (a) or (b) of this section, with units of state or local governments, and with private entities to carry out the collection of DNA samples. An agency may, but need not, collect a DNA sample from an individual if—

(1) Another agency or entity has collected, or will collect, a DNA sample from that individual pursuant to an agreement under this paragraph;

(2) The Combined DNA Index System already contains a DNA analysis with respect to that individual; or

(3) Waiver of DNA-sample collection in favor of collection by another agency is authorized by 42 U.S.C. 14135a(a)(3) or 10 U.S.C. 1565(a)(2).

(f) Each agency required to collect DNA samples under this section shall—

(1) Carry out DNA-sample collection utilizing sample-collection kits provided or other means authorized by the Attorney General, including approved methods of blood draws or buccal swabs;

(2) Furnish each DNA sample collected under this section to the Federal Bureau of Investigation, or to another agency or entity as authorized by the Attorney General, for purposes of analysis and entry of the results of the analysis into the Combined DNA Index System; and

(3) Repeat DNA-sample collection from an individual who remains or becomes again subject to the agency’s jurisdiction or control if informed that a sample collected from the individual does not satisfy the requirements for
(g) The authorization of DNA-sample collection by this section pursuant to Public Law 106-546 does not limit DNA-sample collection by any agency pursuant to any other authority.

Official Citation:


(a) The Federal Bureau of Investigation shall carry out a DNA analysis on each DNA sample furnished to the Federal Bureau of Investigation pursuant to section 3(b) or 4(b) of Public Law 106-54, and shall include the results in the Combined DNA Index System.

(b) The Federal Bureau of Investigation shall include in the Combined DNA Index System the results of each analysis furnished to the Federal Bureau of Investigation pursuant to 10 U.S.C. 1565(b)(2).
SUBPART C—Preservation of Biological Evidence

Source:
Order No. 2762-2005, 70 FR 21957, Apr. 28, 2005, unless otherwise noted.

28 CFR Section 28.21: Purpose.

Section 3600A of title 18 of the United States Code ("section 3600A") requires the Government to preserve biological evidence that was secured in the investigation or prosecution of a Federal offense, if a defendant is under a sentence of imprisonment for such offense, subject to certain limitations and exceptions. The general purpose of this requirement is to preserve biological evidence for possible DNA testing under 18 U.S.C. 3600. Subsection (e) of section 3600A requires the Attorney General to promulgate regulations to implement and enforce section 3600A, including appropriate disciplinary sanctions to ensure that employees comply with such regulations.


(a) Applicability in general.
The requirement of section 3600A to preserve biological evidence applies to evidence that has been retained in cases in which the offense or conviction occurred prior to the enactment of section 3600A or the adoption of this subpart, as well as to evidence secured in pending and future cases.

(b) Limitation to circumstances in which a defendant is under a sentence of imprisonment for the offense.
The requirement of section 3600A to preserve biological evidence secured in the investigation or prosecution of a Federal offense begins to apply when a defendant is convicted and sentenced to imprisonment for the offense, and ceases to apply when the defendant or defendants are released following such imprisonment. The evidence preservation requirement of section 3600A does not apply in the following situations:

(1) Inapplicability at the investigative stage.
The requirement of section 3600A to preserve biological evidence does not apply at the investigative stage of criminal cases, occurring prior to the conviction and sentencing to imprisonment of a defendant. Biological evidence may be collected and preserved in the investigation of Federal offenses prior to the sentencing of a defendant to imprisonment, reflecting sound investigative practice and the need
for evidence in trial proceedings that may result from the investigation, but section 3600A does not govern these activities.

(2) Inapplicability to cases involving only non-incarcerative sentences. The requirement of section 3600A to preserve biological evidence does not apply in cases in which defendants receive only nonincarcerative sentences, such as probation, fines, or payment of restitution.

(3) Inapplicability following release. The requirement of section 3600A to preserve biological evidence ceases to apply when the defendant or defendants are released following imprisonment, either unconditionally or under supervision. The requirement does not apply during any period following the release of the defendant or defendants from imprisonment, even if the defendant or defendants remain on supervised release or parole.

(4) Inapplicability following revocation of release. The requirement of section 3600A to preserve biological evidence applies during a defendant's imprisonment pursuant to the sentence imposed upon conviction of the offense, as opposed to later imprisonment resulting from a violation of release conditions. The requirement does not apply during any period in which the defendant or defendants are imprisoned based on the revocation of probation, supervised release, or parole.

(c) Conditions of preservation. The requirement of section 3600A to preserve biological evidence means that such evidence cannot be destroyed or disposed of under the circumstances in which section 3600A requires its preservation, but does not limit agency discretion concerning the conditions under which biological evidence is maintained or the transfer of biological evidence among different agencies.

28 CFR Section 28.23: Evidence subject to the preservation requirement.

(a) Biological evidence generally. The evidence preservation requirement of section 3600A applies to “biological evidence,” which is defined in section 3600A(b). The covered evidence is sexual assault forensic examination kits under section 3600A(b)(1) and semen, blood, saliva, hair, skin tissue, or other identified biological material under section 3600A(b)(2).

(b) Biological evidence under section 3600A(b)(2).
Biological evidence within the scope of section 3600A(b)(2) is identified biological material that may derive from a perpetrator of the offense, and hence might be capable of shedding light on the question of a defendant's guilt or innocence through DNA testing to determine whether the defendant is the source of the material. In greater detail, evidence within the scope of section 3600A(b)(2) encompasses the following:

(1) **Identified biological material.**
Beyond sexual assault forensic examination kits, which are specially referenced in section 3600A(b)(1), section 3600A requires preservation only of evidence that is detected and identified as semen, blood, saliva, hair, skin tissue, or some other type of biological material. Section 3600A's preservation requirement does not apply to an item of evidence merely because it is known on theoretical grounds that physical things that have been in proximity to human beings almost invariably contain unidentified and imperceptible amounts of their organic matter.

(2) **Material that may derive from a perpetrator of the crime.**
Biological evidence within the scope of section 3600A(b)(2) must constitute “biological material.” In the context of section 3600A, this term does not encompass all possible types of organic matter, but rather refers to organic matter that may derive from the body of a perpetrator of the crime, and hence might be capable of shedding light on a defendant's guilt or innocence by including or excluding the defendant as the source of its DNA.

**Example 1.**
In a murder case in which the victim struggled with the killer, scrapings of skin tissue or blood taken from under the victim's fingernails would constitute biological material in the sense of section 3600A(b)(2), and would be subject to section 3600A's requirement to preserve biological evidence, assuming satisfaction of the statute's other conditions. Such material, which apparently derives from the perpetrator of the crime, could potentially shed light on guilt or innocence through DNA testing under 18 U.S.C. 3600 to determine whether a defendant was the source of this material.

**Example 2.**
Biological material in the sense of section 3600A(b)(2) would not include the body of a murder victim who was shot from a distance, the carcasses of cattle in a meat truck secured in an investigation of the truck's hijacking, a quantity of marijuana seized in a drug trafficking investigation, or articles made from wood or from wool or cotton fiber. While such items of evidence constitute organic matter in a broader sense, they are not biological material within the scope of
section 3600A(b)(2), because they do not derive from the body of a perpetrator of the crime, and hence could not shed light on a defendant's guilt or innocence through DNA testing under 18 U.S.C. 3600 to determine whether the defendant is the source of the evidence.

28 CFR Section 28.24: Exceptions based on the results of judicial proceedings.

Subsection (c) of section 3600A makes the biological evidence preservation requirement inapplicable in two circumstances relating to the results of judicial proceedings:

(a) Judicial denial of DNA testing.
Section 3600A(c)(1) exempts situations in which a court has denied a motion for DNA testing under 18 U.S.C. 3600 and no appeal is pending.

(b) Inclusion of defendant as source.
Section 3600A(c)(5) exempts situations in which there has been DNA testing under 18 U.S.C. 3600 and the results included the defendant as the source of the evidence.

28 CFR Section 28.25: Exceptions based on a defendant's conduct.

Subsection (c) of section 3600A makes the biological evidence preservation requirement inapplicable in two circumstances relating to action (or inaction) by the defendant:

(a) Waiver by defendant.
Section 3600A(c)(2) makes the biological evidence preservation requirement inapplicable if the defendant knowingly and voluntarily waived DNA testing in a court proceeding conducted after the date of enactment, i.e., after October 30, 2004. Hence, for example, if a defendant waives DNA testing in the context of a plea agreement, in a pretrial colloquy with the court, in the course of discovery in pretrial proceedings, or in a postconviction proceeding, and the proceeding in which the waiver occurs takes place after October 30, 2004, the biological evidence preservation requirement of section 3600A does not apply.

(b) Notice to defendant.
(1) Section 3600A(c)(3) makes the biological evidence preservation requirement inapplicable if the defendant is notified that the biological evidence may be destroyed “after a conviction becomes final and the defendant has exhausted all opportunities for direct review of the conviction,” and “the
defendant does not file a motion under section 3600 within 180 days of receipt of the notice.”

(2) Effective notice concerning the possible destruction of biological evidence for purposes of section 3600A(c)(3) cannot be given if the case is pending on direct review of the conviction before a court of appeals or the Supreme Court, if time remains for the defendant to file a notice of appeal from the judgment of conviction in the court of appeals, or if time remains for the defendant to file a petition for certiorari to the Supreme Court following the court of appeals' determination of an appeal of the conviction.

(3) Once direct review has been completed, or the time for seeking direct review has expired, section 3600A(c)(3) allows notice to the defendant that biological evidence may be destroyed. The biological evidence preservation requirement of section 3600A thereafter does not apply, unless the defendant files a motion under 18 U.S.C. 3600 within 180 days of receipt of the notice. Notice to a defendant that biological evidence may be destroyed may be provided by certified mail, and the Federal Bureau of Prisons shall create a record concerning the delivery of such mail to an inmate. To determine whether a defendant has filed a motion under 18 U.S.C. 3600 within 180 days of receipt of such a notice, the agency providing the notice may obtain confirmation of delivery and the date of delivery by inquiry with the Federal Bureau of Prisons, and may ascertain whether the defendant has filed a motion under 18 U.S.C. 3600 within 180 days of that date by checking the records of the district court which entered the judgment of conviction of the defendant for the offense or asking the United States Attorney's office in that district.

**28 CFR Section 28.26: Exceptions based on the nature of the evidence.**

Subsection (c)(4) of section 3600A provides that the section's biological evidence preservation requirement does not apply if “the evidence must be returned to its rightful owner, or is of such a size, bulk, or physical character as to render retention impracticable.” This exception is subject to the condition that the Government must “take[] reasonable measures to remove and preserve portions of the material evidence sufficient to permit future DNA testing.”

(a) Evidence not retained beyond the investigative stage.
Section 3600A(c)(4) has no application if items of the sort it describes—e.g., items that must be returned to the rightful owner, or items that are so large that their retention is impracticable—are not kept until the time when a defendant is convicted and sentenced to imprisonment. Investigative agents may take samples from such items during the investigative stage of the case, in accordance with their judgment about what is needed for purposes of DNA testing or other
evidentiary use, or may conclude that the nature of the items does not warrant taking such samples, and the items themselves may then be returned to the owners or otherwise disposed of prior to the trial, conviction, or sentencing of any defendant. In such cases, section 3600A is inapplicable, because its evidence preservation requirement does not apply at all until a defendant is sentenced to imprisonment, as noted in § 28.22(b)(1).

(b) Evidence not constituting biological material.
It is rarely the case that a bulky item of the sort described in section 3600A(c)(4), or a large part of such an item, constitutes biological evidence as defined in section 3600A(b). If such an item is not biological evidence in the relevant sense, it is outside the scope of section 3600A. For example, the evidence secured in the investigation of a bank robbery may include a stolen car that was used in the getaway, and there may be some item in the car containing biological material that derives from a perpetrator of the crime, such as saliva on a discarded cigarette butt. Even if the vehicle is kept until a defendant is sentenced to imprisonment, section 3600A's preservation requirement would not apply to the vehicle as such, because the vehicle is not biological material. It would be sufficient for compliance with section 3600A to preserve the particular items in the vehicle that contain identified biological material or portions of them that contain the biological material.

(c) Preservation of portions sufficient for DNA testing.
If evidence described in section 3600A(c)(4) is not otherwise exempt from the preservation requirement of section 3600A, and section 3600A(c)(4) is relied on in disposing of such evidence, reasonable measures must be taken to preserve portions of the evidence sufficient to permit future DNA testing. For example, considering a stolen car used in a bank robbery, it may be the case that one of the robbers was shot during the getaway and bled all over the interior of the car. In such a case, if the car is kept until a defendant is sentenced to imprisonment for the crime, there would be extensive biological material in the car that would potentially be subject to section 3600A's requirement to preserve biological evidence. Moreover, the biological material in question could not be fully preserved without retaining the whole car or removing and retaining large amounts of matter from the interior of the car. Section 3600A(c)(4) would be relevant in such a case, given that fully retaining the biological evidence is likely to be impracticable or inconsistent with the rightful owner's entitlement to the return of the vehicle. In such a case, section 3600A(c)(4) could be relied on, and its requirements would be satisfied if samples of the blood were preserved sufficient to permit future DNA testing. Preserving such samples would dispense with any need under section 3600A to retain the vehicle itself or larger portions thereof.
Section 3600A's requirement to preserve biological evidence applies cumulatively with other evidence retention requirements. It does not preempt or supersede any statute, regulation, court order, or other provision of law that may require evidence, including biological evidence, to be preserved.

(a) Disciplinary sanctions. Violations of section 3600A or of this subpart by Government employees shall be subject to the disciplinary sanctions authorized by the rules or policies of their employing agencies for violations of statutory or regulatory requirements.

(b) Criminal sanctions. Violations of section 3600A may also be subject to criminal sanctions as prescribed in subsection (f) of that section. Section 3600A(f) makes it a felony offense, punishable by up to five years of imprisonment, for anyone to knowingly and intentionally destroy, alter, or tamper with biological evidence that is required to be preserved under section 3600A with the intent to prevent that evidence from being subjected to DNA testing or prevent the production or use of that evidence in an official proceeding.

(c) No effect on validity of convictions. Section 3600A's requirements are enforceable through the disciplinary sanctions and criminal sanctions described in paragraphs (a) and (b) of this section. A failure to preserve biological evidence as required by section 3600A does not provide a basis for relief in any postconviction proceeding.
28 CFR PART 29—MOTOR VEHICLE THEFT PREVENTION ACT REGULATIONS

➤ 28 CFR Section 29.1: Purpose.
➤ 28 CFR Section 29.2: Definitions.
➤ 28 CFR Section 29.3: Administration by the Bureau of Justice Assistance.
➤ 28 CFR Section 29.4: Election to participate by states and localities.
➤ 28 CFR Section 29.5: Notification of law enforcement officials.
➤ 28 CFR Section 29.6: Limited participation by states and localities permitted.
➤ 28 CFR Section 29.7: Withdrawal from the program by states and localities.
➤ 28 CFR Section 29.8: Motor vehicle owner participation.
➤ 28 CFR Section 29.9: Motor vehicles for hire.
➤ 28 CFR Section 29.10: Owner withdrawal from the program.
➤ 28 CFR Section 29.11: Sale or other transfer of an enrolled vehicle.
➤ 28 CFR Section 29.12: Specified conditions under which stops may be authorized.
➤ 28 CFR Section 29.13: No new conditions without consent.

Authority:

Source:
61 FR 40725, Aug. 6, 1996, unless otherwise noted.
28 CFR Section 29.1: Purpose.

(a) The purpose of this part is to implement the Motor Vehicle Theft Prevention Act, 42 U.S.C. 14171, which requires the Attorney General to develop, in cooperation with the states, a national voluntary motor vehicle theft prevention program. The program will be implemented by states and localities, at their sole option.

(b) Under this program, individual motor vehicle owners voluntarily sign a consent form in which the owner

(1) Indicates that the identified vehicle is not normally operated under certain specified conditions and

(2) Agrees to display a program decal or license plate on the vehicle and to permit law enforcement officials in any jurisdiction to stop the motor vehicle if it is being operated under specified conditions and take reasonable steps to determine whether the vehicle is being operated by or with the permission of the owner.

(c) The regulations set forth in this part establish the conditions under which an owner may consent to having his or her vehicle stopped and the manner in which a State or locality may elect to participate.

28 CFR Section 29.2: Definitions.

For the purposes of this part:

(a) The Act
or the MVTPA means the Motor Vehicle Theft Prevention Act.

(b) Owner
means the person or persons whose name(s) appear(s) on the certificate of title or to whom the car is registered. In the instance of a new vehicle awaiting sale or lease or in the instance of a used vehicle where the title has been assigned to a dealership, the term “owner” shall be construed to mean new and used automobile dealerships.

(c) The Program
refers to the National Voluntary Motor Vehicle Theft Prevention Program implemented pursuant to the Motor Vehicle Prevention Act.
28 CFR Section 29.3: Administration by the Bureau of Justice Assistance.

The Director of the Bureau of Justice Assistance shall administer this Program and shall issue guidelines governing the operational aspects of it, including the design and production of a standardized, universally recognizable MVTPA reflective decal, as well as model consent and registration forms.

28 CFR Section 29.4: Election to participate by states and localities.

(a) Any State or locality that wishes to participate in the program shall register with the BJA and request program enrollment materials. Registration forms will be available upon request. Participation in the program is wholly voluntary on the part of the State or locality.

(b) By electing to participate in the program, a State or locality agrees to do the following:

(1) Make program enrollment materials, including consent forms, available to interested motor vehicle owners;

(2) Collect completed consent forms;

(3) Provide enrolled motor vehicle owners with the decal(s), and license plate(s) applicable to their program condition or conditions and instructions governing program participation;

(4) Take the necessary steps to authorize law enforcement officials to stop motor vehicles enrolled in the program; and

(5) Comply with any other regulation(s) or guideline(s) governing participation in this program.

28 CFR Section 29.5: Notification of law enforcement officials.

In addition to the actions enumerated in § 29.4(b), as a condition of participating in the program, a State or locality must agree to take reasonable steps to ensure that law enforcement officials under its jurisdiction are familiar with the program and with the conditions under which motor vehicles may be stopped.
28 CFR Section 29.6: Limited participation by states and localities permitted.

A State or locality need not authorize the stopping of motor vehicles under all sets of conditions specified under the program in order to participate in the program.

28 CFR Section 29.7: Withdrawal from the program by states and localities.

Any participating State or locality may withdraw from the program at any time by sending written notification to BJA and by notifying participating owners individually by mail of the decision to withdraw.

28 CFR Section 29.8: Motor vehicle owner participation.

In order to participate in this program, the owner(s) of a motor vehicle must sign a program consent form and register with a participating State or locality. If the vehicle is registered to more than one person, both owners must sign the consent form. By enrolling in the federal program, the owner(s) of the motor vehicle—

(a) State(s) that the vehicle is not normally operated under the specified conditions; and

(b) Agree(s) to:

(1) Display the program decals or devices on the owner's vehicle;

(2) Permit law enforcement officials in any State or locality to stop the motor vehicle if the vehicle is being operated under the specified conditions and take reasonable steps to determine whether the vehicle is being operated by or with the permission of the owner;

(3) Expressly advise any borrower of the vehicle of the existence of this agreement, and that such user will be subject to being stopped by law enforcement officials if the vehicle is being operated under the specified condition(s) even if the officials have no other basis for believing the vehicle is being operated unlawfully; and

(4) Comply with any other regulation(s) or guideline(s) governing participation in this program.
28 CFR Section 29.9: Motor vehicles for hire.

(a) Any person who is in the business of renting or leasing motor vehicles and who rents or leases a motor vehicle on which a program decal or device is affixed shall notify the person to whom the motor vehicle is rented or leased about the program, prior to transferring possession of the vehicle.

(b) The notice required by this section shall be printed in bold type in the rental or lease agreement, and on the envelope in which the rental agreement is placed. The notice provision in the rental or lease agreement must utilize a larger font than the standard type in the agreement. The notice must state that the motor vehicle may be stopped by law enforcement officials if it is operated under the conditions specified by the program in which the car is enrolled even if the officials have no other basis for believing that the vehicle is being operated unlawfully.

(c) Failure to provide the notice required by this section to a renter or lessee may result in the assessment of a civil penalty by the Assistant Attorney General, Civil Division, or his or her designee, of an amount not to exceed $5,000. No penalty shall be assessed unless the person charged has been given notice and an opportunity for a hearing of such charge.

28 CFR Section 29.10: Owner withdrawal from the program.

An owner may withdraw from the program at any time by completely removing the program decal and changing the license plate if necessary. The owner is also encouraged to notify the participating agency in writing of such withdrawal.

28 CFR Section 29.11: Sale or other transfer of an enrolled vehicle.

Upon the transferral of ownership of an enrolled vehicle, the transferring owner must completely remove the program decals, change the license plate(s) if necessary, and is encouraged to notify the participating agency in writing of the transfer of ownership of the vehicle.

28 CFR Section 29.12: Specified conditions under which stops may be authorized.
A motor vehicle owner may voluntarily enroll his or her vehicle(s) and give written consent to law enforcement official to stop the vehicle if it is being operated under any or all the conditions set forth in this section. For each condition, the owner(s) must grant consent and affix a separate decal, device, or license plate.

(a) Time.
A motor vehicle owner may authorize law enforcement officers to stop the enrolled vehicle if it is being operated between the hours of 1:00 AM and 5:00 AM. By enrolling in a program with this condition, the owner must state that the vehicle is not normally operated between the specified hours, and that the owner understands that the operation of the vehicle between those hours provides sufficient grounds for a law enforcement officer to reasonably believe that the vehicle is not being operated by or with the consent of the owner, even if the law enforcement official has no other basis for believing that the vehicle is being operated unlawfully.

(b) Border crossing or port entry.
A motor vehicle owner may authorize law enforcement officers to stop the enrolled vehicle if it crosses, is about to cross or is about to be transported across a United States land border, or if it enters a United States port. For purposes of this section, the phrase ―about to cross a United States land border‖ means the vehicle is operated or transported within one mile of a United States land border. Participating States or localities may implement this provision in accordance with local conditions, provided that a participating State or locality may not extend the applicable geographic area beyond one mile from the United States land border. By enrolling in a program with this condition, the owner must state that the vehicle is not normally driven across a border or into a port, and that the owner understands that the operation or transport of the vehicle within a mile of a United States land border or into a port provides sufficient grounds for a law enforcement officer to believe that the vehicle is not being operated by or with the consent of the owner even if the law enforcement officer has no other basis for believing that the vehicle is being operated unlawfully.

28 CFR Section 29.13: No new conditions without consent.

After the program has begun, new conditions under which a vehicle may be stopped may only be added to an existing program if the owner consents to the new condition or conditions.

Page 632
28 CFR PART 45—EMPLOYEE RESPONSIBILITIES

- 28 CFR Section 45.1: Cross-reference to ethical standards and financial disclosure regulations.
- 28 CFR Section 45.2: Disqualification arising from personal or political relationship.
- 28 CFR Section 45.4: Personal use of Government property.
- 28 CFR Section 45.10: Procedures to promote compliance with crime victims' rights obligations.
- 28 CFR Section 45.12: Reporting to the Department of Justice Office of Professional Responsibility.
- 28 CFR Section 45.13: Duty to cooperate in an official investigation.

Authority:
28 CFR Section 45.1: Cross-reference to ethical standards and financial disclosure regulations.

Employees of the Department of Justice are subject to the executive branch-wide Standards of Ethical Conduct at 5 CFR part 2635, the Department of Justice regulations at 5 CFR part 3801 which supplement the executive branch-wide standards, the executive branch-wide financial disclosure regulations at 5 CFR part 2634 and the executive branch-wide employee responsibilities and conduct regulations at 5 CFR part 735.

Official Citation:
[61 FR 59815, Nov. 25, 1996]

28 CFR Section 45.2: Disqualification arising from personal or political relationship.

(a) Unless authorized under paragraph (b) of this section, no employee shall participate in a criminal investigation or prosecution if he has a personal or political relationship with:

(1) Any person or organization substantially involved in the conduct that is the subject of the investigation or prosecution; or

(2) Any person or organization which he knows has a specific and substantial interest that would be directly affected by the outcome of the investigation or prosecution.

(b) An employee assigned to or otherwise participating in a criminal investigation or prosecution who believes that his participation may be prohibited by paragraph (a) of this section shall report the matter and all attendant facts and circumstances to his supervisor at the level of section chief or the equivalent or higher. If the supervisor determines that a personal or political relationship exists between the employee and a person or organization described in paragraph (a) of this section, he shall relieve the employee from participation unless he determines further, in writing, after full consideration of all the facts and circumstances, that:

(1) The relationship will not have the effect of rendering the employee's service less than fully impartial and professional; and

(2) The employee's participation would not create an appearance of a conflict of interest likely to affect the public perception of the integrity of the investigation or prosecution.
(c) For the purposes of this section:

(1) **Political relationship**

means a close identification with an elected official, a candidate (whether or not successful) for elective, public office, a political party, or a campaign organization, arising from service as a principal adviser thereto or a principal official thereof; and

(2) **Personal relationship**

means a close and substantial connection of the type normally viewed as likely to induce partiality. An employee is presumed to have a personal relationship with his father, mother, brother, sister, child and spouse. Whether relationships (including friendships) of an employee to other persons or organizations are “personal” must be judged on an individual basis with due regard given to the subjective opinion of the employee.

(d) This section pertains to agency management and is not intended to create rights enforceable by private individuals or organizations.

**Official Citation:**


28 CFR Section 45.3: Disciplinary proceedings under 18 U.S.C. 207(j).

(a) Upon a determination by the Assistant Attorney General in charge of the Criminal Division (Assistant Attorney General), after investigation, that there is reasonable cause to believe that a former officer or employee, including a former special Government employee, of the Department of Justice (former departmental employee) has violated 18 U.S.C. 207 (a), (b) or (c), the Assistant Attorney General shall cause a copy of written charges of the violation(s) to be served upon such individual, either personally or by registered mail. The charges shall be accompanied by a notice to the former departmental employee to show cause within a specified time of not less than 30 days after receipt of the notice why he or she should not be prohibited from engaging in representational activities in relation to matters pending in the Department of Justice, as authorized by 18 U.S.C. 207(j), or subjected to other appropriate disciplinary action under that statute. The notice to show cause shall include:
(1) A statement of allegations, and their basis, sufficiently detailed to enable the former departmental employee to prepare an adequate defense,

(2) Notification of the right to a hearing, and

(3) An explanation of the method by which a hearing may be requested.

(b) If a former departmental employee who submits an answer to the notice to show cause does not request a hearing or if the Assistant Attorney General does not receive an answer within five days after the expiration of the time prescribed by the notice, the Assistant Attorney General shall forward the record, including the report(s) of investigation, to the Attorney General. In the case of a failure to answer, such failure shall constitute a waiver of defense.

(c) Upon receipt of a former departmental employee's request for a hearing, the Assistant Attorney General shall notify him or her of the time and place thereof, giving due regard both to such person's need for an adequate period to prepare a suitable defense and an expeditious resolution of allegations that may be damaging to his or her reputation.

(d) The presiding officer at the hearing and any related proceedings shall be a federal administrative law judge or other federal official with comparable duties. He shall insure that the former departmental employee has, among others, the rights:

(1) To self-representation or representation by counsel,

(2) To introduce and examine witnesses and submit physical evidence,

(3) To confront and cross-examine adverse witnesses,

(4) To present oral argument, and

(5) To a transcript or recording of the proceedings, upon request.

(e) The Assistant Attorney General shall designate one or more officers or employees of the Department of Justice to present the evidence against the former departmental employee and perform other functions incident to the proceedings.

(f) A decision adverse to the former departmental employee must be sustained by substantial evidence that he violated 18 U.S.C. 207 (a), (b) or (c).

(g) The presiding officer shall issue an initial decision based exclusively on the transcript of testimony and exhibits, together with all papers and requests filed in
the proceeding, and shall set forth in the decision findings and conclusions, supported by reasons, on the material issues of fact and law presented on the record.

(h) Within 30 days after issuance of the initial decision, either party may appeal to the Attorney General, who in that event shall issue the final decision based on the record of the proceedings or those portions thereof cited by the parties to limit the issues. If the final decision modifies or reverses the initial decision, the Attorney General shall specify the findings of fact and conclusions of law that vary from those of the presiding officer.

(i) If a former departmental employee fails to appeal from an adverse initial decision within the prescribed period of time, the presiding officer shall forward the record of the proceedings to the Attorney General.

(j) In the case of a former departmental employee who filed an answer to the notice to show cause but did not request a hearing, the Attorney General shall make the final decision on the record submitted to him by the Assistant Attorney General pursuant to subsection (b) of this section.

(k) The Attorney General, in a case where:

(1) The defense has been waived,

(2) The former departmental employee has failed to appeal from an adverse initial decision, or

(3) The Attorney General has issued a final decision that the former departmental employee violated 18 U.S.C. 207 (a), (b) or (c),

may issue an order:

(i) Prohibiting the former departmental employee from making, on behalf of any other person (except the United States), any informal or formal appearance before, or, with the intent to influence, any oral or written communication to, the Department of Justice on a pending matter of business for a period not to exceed five years, or

(ii) Prescribing other appropriate disciplinary action.

(l) An order issued under either paragraph (k)(3) (i) or (ii) of this section may be supplemented by a directive to officers and employees of the Department of Justice not to engage in conduct in relation to the former departmental employee that would contravene such order.

Official Citation:
28 CFR Section 45.4: Personal use of Government property.

(a) Employees may use Government property only for official business or as authorized by the Government. See 5 CFR 2635.101(b)(9), 2635.704(a). The following uses of Government office and library equipment and facilities are hereby authorized:

(1) Personal uses that involve only negligible expense (such as electricity, ink, small amounts of paper, and ordinary wear and tear); and

(2) Limited personal telephone/fax calls to locations within the office's commuting area, or that are charged to non-Government accounts.

(b) The foregoing authorization does not override any statutes, rules, or regulations governing the use of specific types of Government property (e.g., internal Departmental policies governing the use of electronic mail; and 41 CFR (FPMR) 101-35.201, governing the authorized use of long-distance telephone services), and may be revoked or limited at any time by any supervisor or component for any business reason.

(c) In using Government property, employees should be mindful of their responsibility to protect and conserve such property and to use official time in an honest effort to perform official duties. See 5 CFR 2635.101(b)(9), 2635.704(a), 2635.705(a).

Official Citation:
means a person directly and proximately harmed as a result of the commission of a Federal offense or an offense in the District of Columbia. In the case of a crime victim who is under 18 years of age, incompetent, incapacitated, or deceased, the legal guardians of the crime victim or the representatives of the crime victim's estate, family members, or any other persons appointed as suitable by the court, may assume the crime victim's rights, but in no event shall the defendant be named as such guardian or representative.

Crime victims' rights

means those rights provided in 18 U.S.C. 3771.

Employee of the Department of Justice

means an attorney, investigator, law enforcement officer, or other personnel employed by any division or office of the Department of Justice whose regular course of duties includes direct interaction with crime victims, not including a contractor.

Office of the Department of Justice

means a component of the Department of Justice whose employees directly interact with crime victims in the regular course of their duties.

(b)
The Attorney General shall designate an official within the Executive Office for United States Attorneys (EOUSA) to receive and investigate complaints alleging the failure of Department of Justice employees to provide rights to crime victims under 18 U.S.C. 3771. The official shall be called the Department of Justice Victims' Rights Ombudsman (VRO). The VRO shall then designate, in consultation with each office of the Department of Justice, an official in each office to serve as the initial point of contact (POC) for complainants.

(c) Complaint process.

(1) Complaints must be submitted in writing to the POC of the relevant office or offices of the Department of Justice. If a complaint alleges a violation that would create a conflict of interest for the POC to investigate, the complaint shall be forwarded by the POC immediately to the VRO.

(2) Complaints shall contain, to the extent known to, or reasonably available to, the victim, the following information:
(i) The name and personal contact information of the crime victim who allegedly was denied one or more crime victims' rights;

(ii) The name and contact information of the Department of Justice employee who is the subject of the complaint, or other identifying information if the complainant is not able to provide the name and contact information;

(iii) The district court case number;

(iv) The name of the defendant in the case;

(v) The right or rights listed in 18 U.S.C. 3771 that the Department of Justice employee is alleged to have violated; and

(vi) Specific information regarding the circumstances of the alleged violation sufficient to enable the POC to conduct an investigation, including, but not limited to: The date of the alleged violation; an explanation of how the alleged violation occurred; whether the complainant notified the Department of Justice employee of the alleged violation; how and when such notification was provided to the Department of Justice employee; and actions taken by the Department of Justice employee in response to the notification.

(3) Complaints must be submitted within 60 days of the victim’s knowledge of a violation, but not more than one year after the actual violation.

(4)(i) In response to a complaint that provides the information required under paragraph (c)(2) of this section and that contains specific and credible information that demonstrates that one or more crime victims' rights listed in 18 U.S.C. 3771 may have been violated by a Department of Justice employee or office, the POC shall investigate the allegation(s) in the complaint within a reasonable period of time.

(ii) The POC shall report the results of the investigation to the VRO.

(5) Upon receipt of the POC's report of the investigation, the VRO shall determine whether to close the complaint without further action, whether further investigation is warranted, or whether action in accordance with paragraphs (d) or (e) of this section is necessary.

(6) Where the VRO concludes that further investigation is warranted, he may conduct such further investigation. Upon conclusion of the investigation, the VRO may close the complaint if he determines that no further action is warranted or may take action under paragraph (d) or (e) of this section.

(7) The VRO shall be the final arbiter of the complaint.
(8) A complainant may not seek judicial review of the VRO’s determination regarding the complaint.

(9) To the extent permissible in accordance with the Privacy Act and other relevant statutes and regulations regarding release of information by the Federal government, the VRO, in his discretion, may notify the complainant of the result of the investigation.

(10) The POC and the VRO shall refer to the Office of the Inspector General and to the Office of Professional Responsibility any matters that fall under those offices' respective jurisdictions that come to light in an investigation.

(d) If the VRO finds that an employee or office of the Department of Justice has failed to provide a victim with a right to which the victim is entitled under 18 U.S.C. 3771, but not in a willful or wanton manner, he shall require such employee or office of the Department of Justice to undergo training on victims' rights.

(e) Disciplinary procedures.

(1) If, based on the investigation, the VRO determines that a Department of Justice employee has wantonly or willfully failed to provide the complainant with a right listed in 18 U.S.C. 3771, the VRO shall recommend, in conformity with laws and regulations regarding employee discipline, a range of disciplinary sanctions to the head of the office of the Department of Justice in which the employee is located, or to the official who has been designated by Department of Justice regulations and procedures to take action on disciplinary matters for that office. The head of that office of the Department of Justice, or the other official designated by Department of Justice regulations and procedures to take action on disciplinary matters for that office, shall be the final decision-maker regarding the disciplinary sanction to be imposed, in accordance with applicable laws and regulations.

(2) Disciplinary sanctions available under paragraph (e)(1) of this section include all sanctions provided under the Department of Justice Human Resources Order, 1200.1.

Official Citation:
[70 FR 69653, Nov. 17, 2005]

Department of Justice employees have a duty to, and shall, report to the Department of Justice Office of the Inspector General, or to their supervisor or their component's internal affairs office for referral to the Office of the Inspector General:

(a) Any allegation of waste, fraud, or abuse in a Department program or activity;

(b) Any allegation of criminal or serious administrative misconduct on the part of a Department employee (except those allegations of misconduct that are required to be reported to the Department of Justice Office of Professional Responsibility pursuant to § 45.12); and

(c) Any investigation of allegations of criminal misconduct against any Department employee.

Official Citation:
[Order No. 2835-2006, 71 FR 54414, Sept. 15, 2006]

28 CFR Section 45.12: Reporting to the Department of Justice Office of Professional Responsibility.

Department employees have a duty to, and shall, report to the Department of Justice Office of Professional Responsibility (DOJ-OPR), or to their supervisor, or their component’s internal affairs office for referral to DOJ-OPR, any allegations of misconduct by a Department attorney that relate to the exercise of the attorney's authority to investigate, litigate or provide legal advice, as well as allegations of misconduct by law enforcement personnel when such allegations are related to allegations of attorney misconduct within the jurisdiction of DOJ-OPR.

Official Citation:
[Order No. 2835-2006, 71 FR 54414, Sept. 15, 2006]

28 CFR Section 45.13: Duty to cooperate in an official investigation.

Department employees have a duty to, and shall, cooperate fully with the Office of the Inspector General and Office of Professional Responsibility, and shall respond to questions posed during the course of an investigation upon being informed that their statement will not be used to incriminate them in a criminal proceeding. Refusal to cooperate could lead to disciplinary action.
Official Citation:
[Order No. 2835-2006, 71 FR 54414, Sept. 15, 2006]
28 CFR PART 46—PROTECTION OF HUMAN SUBJECTS

- 28 CFR Section 46.101: To what does this policy apply?
- 28 CFR Section 46.102: Definitions.
- 28 CFR Section 46.103: Assuring compliance with this policy—research conducted or supported by any Federal Department or Agency.
- 28 CFR Section 46.104-46.106: [Reserved]
- 28 CFR Section 46.108: IRB functions and operations.
- 28 CFR Section 46.109: IRB review of research.
- 28 CFR Section 46.110: Expedited review procedures for certain kinds of research involving no more than minimal risk, and for minor changes in approved research.
- 28 CFR Section 46.111: Criteria for IRB approval of research.
- 28 CFR Section 46.112: Review by institution.
- 28 CFR Section 46.113: Suspension or termination of IRB approval of research.
- 28 CFR Section 46.114: Cooperative research.
- 28 CFR Section 46.115: IRB records.
- 28 CFR Section 46.116: General requirements for informed consent.
- 28 CFR Section 46.117: Documentation of informed consent.
- 28 CFR Section 46.118: Applications and proposals lacking definite plans for involvement of human subjects.
- 28 CFR Section 46.119: Research undertaken without the intention of involving human subjects.
- 28 CFR Section 46.120: Evaluation and disposition of applications and proposals for research to be conducted or supported by a Federal Department or Agency.
- 28 CFR Section 46.121: [Reserved]
- 28 CFR Section 46.123: Early termination of research support: Evaluation of applications and proposals.
- 28 CFR Section 46.124: Conditions.

Authority:

Source:
56 FR 28012, 28020, June 18, 1991, unless otherwise noted.
28 CFR Section 46.101: To what does this policy apply?

(a) Except as provided in paragraph (b) of this section, this policy applies to all research involving human subjects conducted, supported or otherwise subject to regulation by any federal department or agency which takes appropriate administrative action to make the policy applicable to such research. This includes research conducted by federal civilian employees or military personnel, except that each department or agency head may adopt such procedural modifications as may be appropriate from an administrative standpoint. It also includes research conducted, supported, or otherwise subject to regulation by the federal government outside the United States.

(1) Research that is conducted or supported by a federal department or agency, whether or not it is regulated as defined in § 46.102(e), must comply with all sections of this policy.

(2) Research that is neither conducted nor supported by a federal department or agency but is subject to regulation as defined in § 46.102(e) must be reviewed and approved, in compliance with § 46.101, § 46.102, and § 46.107 through § 46.117 of this policy, by an institutional review board (IRB) that operates in accordance with the pertinent requirements of this policy.

(b) Unless otherwise required by department or agency heads, research activities in which the only involvement of human subjects will be in one or more of the following categories are exempt from this policy:

(1) Research conducted in established or commonly accepted educational settings, involving normal educational practices, such as (i) research on regular and special education instructional strategies, or (ii) research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods.

(2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:

(i) Information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and

(ii) Any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.
(3) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior that is not exempt under paragraph (b)(2) of this section, if:

(i) The human subjects are elected or appointed public officials or candidates for public office; or

(ii) Federal statute(s) require(s) without exception that the confidentiality of the personally identifiable information will be maintained throughout the research and thereafter.

(4) Research, involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects.

(5) Research and demonstration projects which are conducted by or subject to the approval of department or agency heads, and which are designed to study, evaluate, or otherwise examine:

(i) Public benefit or service programs;

(ii) Procedures for obtaining benefits or services under those programs;

(iii) Possible changes in or alternatives to those programs or procedures; or

(iv) Possible changes in methods or levels of payment for benefits or services under those programs.

(6) Taste and food quality evaluation and consumer acceptance studies,

(i) If wholesome foods without additives are consumed or

(ii) If a food is consumed that contains a food ingredient at or below the level and for a use found to be safe, or agricultural chemical or environmental contaminant at or below the level found to be safe, by the Food and Drug Administration or approved by the Environmental Protection Agency or the Food Safety and Inspection Service of the U.S. Department of Agriculture.

(c) Department or agency heads retain final judgment as to whether a particular activity is covered by this policy.
(d) Department or agency heads may require that specific research activities or classes of research activities conducted, supported, or otherwise subject to regulation by the department or agency but not otherwise covered by this policy, comply with some or all of the requirements of this policy.

(e) Compliance with this policy requires compliance with pertinent federal laws or regulations which provide additional protections for human subjects.

(f) This policy does not affect any state or local laws or regulations which may otherwise be applicable and which provide additional protections for human subjects.

(g) This policy does not affect any foreign laws or regulations which may otherwise be applicable and which provide additional protections to human subjects of research.

(h) When research covered by this policy takes place in foreign countries, procedures normally followed in the foreign countries to protect human subjects may differ from those set forth in this policy. (An example is a foreign institution which complies with guidelines consistent with the World Medical Assembly Declaration (Declaration of Helsinki amended 1989) issued either by sovereign states or by an organization whose function for the protection of human research subjects is internationally recognized.) In these circumstances, if a department or agency head determines that the procedures prescribed by the institution afford protections that are at least equivalent to those provided in this policy, the department or agency head may approve the substitution of the foreign procedures in lieu of the procedural requirements provided in this policy. Except when otherwise required by statute, Executive Order, or the department or agency head, notices of these actions as they occur will be published in the Federal Register or will be otherwise published as provided in department or agency procedures.

(i) Unless otherwise required by law, department or agency heads may waive the applicability of some or all of the provisions of this policy to specific research activities or classes of research activities otherwise covered by
this policy. Except when otherwise required by statute or Executive Order, the department or agency head shall forward advance notices of these actions to the Office for Human Research Protections, Department of Health and Human Services (HHS), or any successor office, and shall also publish them in the Federal Register or in such other manner as provided in department or agency procedures.\(^7\)

**Official Citation:**

---

28 CFR Section 46.102: Definitions.

(a) Department or agency head
means the head of any federal department or agency and any other officer or employee of any department or agency to whom authority has been delegated.

(b) Institution
means any public or private entity or agency (including federal, state, and other agencies).

(c) Legally authorized representative
means an individual or judicial or other body authorized under applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure(s) involved in the research.

(d) Research

---

\(^7\) Institutions with HHS-approved assurances on file will abide by provisions of title 45 CFR part 46 subparts A-D. Some of the other Departments and Agencies have incorporated all provisions of title 45 CFR part 46 into their policies and procedures as well. However, the exemptions at 45 CFR 46.101(b) do not apply to research involving prisoners, subpart C. The exemption at 45 CFR 46.101(b)(2), for research involving survey or interview procedures or observation of public behavior, does not apply to research with children, subpart D, except for research involving observations of public behavior when the investigator(s) do not participate in the activities being observed.
means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes. For example, some demonstration and service programs may include research activities.

(e) Research subject to regulation, and similar terms are intended to encompass those research activities for which a federal department or agency has specific responsibility for regulating as a research activity, (for example, Investigational New Drug requirements administered by the Food and Drug Administration). It does not include research activities which are incidentally regulated by a federal department or agency solely as part of the department’s or agency’s broader responsibility to regulate certain types of activities whether research or non-research in nature (for example, Wage and Hour requirements administered by the Department of Labor).

(f) Human subject means a living individual about whom an investigator (whether professional or student) conducting research obtains

1. Data through intervention or interaction with the individual, or

2. Identifiable private information.

Intervention includes both physical procedures by which data are gathered (for example, venipuncture) and manipulations of the subject or the subject's environment that are performed for research purposes. Interaction includes communication or interpersonal contact between investigator and subject. Private information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.

(g) IRB means an institutional review board established in accord with and for the purposes expressed in this policy.
(h) IRB approval
means the determination of the IRB that the research has been reviewed and may be conducted at an institution within the constraints set forth by the IRB and by other institutional and federal requirements.

(i) Minimal risk
means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

(j) Certification
means the official notification by the institution to the supporting department or agency, in accordance with the requirements of this policy, that a research project or activity involving human subjects has been reviewed and approved by an IRB in accordance with an approved assurance.

28 CFR Section 46.103: Assuring compliance with this policy—research conducted or supported by any Federal Department or Agency.

(a) Each institution engaged in research which is covered by this policy and which is conducted or supported by a federal department or agency shall provide written assurance satisfactory to the department or agency head that it will comply with the requirements set forth in this policy. In lieu of requiring submission of an assurance, individual department or agency heads shall accept the existence of a current assurance, appropriate for the research in question, on file with the Office for Human Research Protections, HHS, or any successor office, and approved for federalwide use by that office. When the existence of an HHS-approved assurance is accepted in lieu of requiring submission of an assurance, reports (except certification) required by this policy to be made to department and agency heads shall also be made to the Office for Human Research Protections, HHS, or any successor office.

(b) Departments and agencies will conduct or support research covered by this policy only if the institution has an assurance approved as provided in this section, and only if the institution has certified to the department or agency head that the research has been reviewed and approved by an IRB provided for in the assurance, and will be subject to continuing review by the IRB. Assurances applicable to federally supported or conducted research shall at a minimum include:
(1) A statement of principles governing the institution in the discharge of its responsibilities for protecting the rights and welfare of human subjects of research conducted at or sponsored by the institution, regardless of whether the research is subject to federal regulation. This may include an appropriate existing code, declaration, or statement of ethical principles, or a statement formulated by the institution itself. This requirement does not preempt provisions of this policy applicable to department- or agency-supported or regulated research and need not be applicable to any research exempted or waived under § 46.101 (b) or (i).

(2) Designation of one or more IRBs established in accordance with the requirements of this policy, and for which provisions are made for meeting space and sufficient staff to support the IRB's review and recordkeeping duties.

(3) A list of IRB members identified by name; earned degrees; representative capacity; indications of experience such as board certifications, licenses, etc., sufficient to describe each member’s chief anticipated contributions to IRB deliberations; and any employment or other relationship between each member and the institution; for example: full-time employee, part-time employee, member of governing panel or board, stockholder, paid or unpaid consultant. Changes in IRB membership shall be reported to the department or agency head, unless in accord with § 46.103(a) of this policy, the existence of an HHS-approved assurance is accepted. In this case, change in IRB membership shall be reported to the Office for Human Research Protections, HHS, or any successor office.

(4) Written procedures which the IRB will follow (i) for conducting its initial and continuing review of research and for reporting its findings and actions to the investigator and the institution; (ii) for determining which projects require review more often than annually and which projects need verification from sources other than the investigators that no material changes have occurred since previous IRB review; and (iii) for ensuring prompt reporting to the IRB of proposed changes in a research activity, and for ensuring that such changes in approved research, during the period for which IRB approval has already been given, may not be initiated without IRB review and approval except when necessary to eliminate apparent immediate hazards to the subject.

(5) Written procedures for ensuring prompt reporting to the IRB, appropriate institutional officials, and the department or agency head of (i) any unanticipated problems involving risks to subjects or others or any serious or continuing noncompliance with this policy or the requirements or determinations of the IRB and (ii) any suspension or termination of IRB approval.

(c) The assurance shall be executed by an individual authorized to act for the institution and to assume on behalf of the institution the obligations imposed by this policy and shall be filed in such form and manner as the department or agency head prescribes.
(d) The department or agency head will evaluate all assurances submitted in accordance with this policy through such officers and employees of the department or agency and such experts or consultants engaged for this purpose as the department or agency head determines to be appropriate. The department or agency head's evaluation will take into consideration the adequacy of the proposed IRB in light of the anticipated scope of the institution's research activities and the types of subject populations likely to be involved, the appropriateness of the proposed initial and continuing review procedures in light of the probable risks, and the size and complexity of the institution.

(e) On the basis of this evaluation, the department or agency head may approve or disapprove the assurance, or enter into negotiations to develop an approvable one. The department or agency head may limit the period during which any particular approved assurance or class of approved assurances shall remain effective or otherwise condition or restrict approval.

(f) Certification is required when the research is supported by a federal department or agency and not otherwise exempted or waived under §46.101 (b) or (i). An institution with an approved assurance shall certify that each application or proposal for research covered by the assurance and by §46.103 of this Policy has been reviewed and approved by the IRB. Such certification must be submitted with the application or proposal or by such later date as may be prescribed by the department or agency to which the application or proposal is submitted. Under no condition shall research covered by §46.103 of the Policy be supported prior to receipt of the certification that the research has been reviewed and approved by the IRB. Institutions without an approved assurance covering the research shall certify within 30 days after receipt of a request for such a certification from the department or agency, that the application or proposal has been approved by the IRB. If the certification is not submitted within these time limits, the application or proposal may be returned to the institution.

(Approved by the Office of Management and Budget under Control Number 0990-0260)

**Official Citation:**

28 CFR Section 46.107: IRB membership.

(a) Each IRB shall have at least five members, with varying backgrounds to promote complete and adequate review of research activities commonly conducted by the institution. The IRB shall be sufficiently qualified through the experience and expertise of its members, and the diversity of the members, including consideration of race, gender, and cultural backgrounds and sensitivity to such issues as community attitudes, to promote respect for its advice and counsel in safeguarding the rights and welfare of human subjects. In addition to possessing the professional competence necessary to review specific research activities, the IRB shall be able to ascertain the acceptability of proposed research in terms of institutional commitments and regulations, applicable law, and standards of professional conduct and practice. The IRB shall therefore include persons knowledgeable in these areas. If an IRB regularly reviews research that involves a vulnerable category of subjects, such as children, prisoners, pregnant women, or handicapped or mentally disabled persons, consideration shall be given to the inclusion of one or more individuals who are knowledgeable about and experienced in working with these subjects.

(b) Every nondiscriminatory effort will be made to ensure that no IRB consists entirely of men or entirely of women, including the institution's consideration of qualified persons of both sexes, so long as no selection is made to the IRB on the basis of gender. No IRB may consist entirely of members of one profession.

(c) Each IRB shall include at least one member whose primary concerns are in scientific areas and at least one member whose primary concerns are in nonscientific areas.

(d) Each IRB shall include at least one member who is not otherwise affiliated with the institution and who is not part of the immediate family of a person who is affiliated with the institution.

(e) No IRB may have a member participate in the IRB’s initial or continuing review of any project in which the member has a conflicting interest, except to provide information requested by the IRB.

(f) An IRB may, in its discretion, invite individuals with competence in special areas to assist in the review of issues which require expertise beyond or in addition to that available on the IRB. These individuals may not vote with the IRB.

28 CFR Section 46.108: IRB functions and operations.

In order to fulfill the requirements of this policy each IRB shall:
(a) Follow written procedures in the same detail as described in § 46.103(b)(4) and, to the extent required by, § 46.103(b)(5).

(b) Except when an expedited review procedure is used (see § 46.110), review proposed research at convened meetings at which a majority of the members of the IRB are present, including at least one member whose primary concerns are in nonscientific areas. In order for the research to be approved, it shall receive the approval of a majority of those members present at the meeting.

28 CFR Section 46.109: IRB review of research.

(a) An IRB shall review and have authority to approve, require modifications in (to secure approval), or disapprove all research activities covered by this policy.

(b) An IRB shall require that information given to subjects as part of informed consent is in accordance with § 46.116. The IRB may require that information, in addition to that specifically mentioned in § 46.116, be given to the subjects when in the IRB's judgment the information would meaningfully add to the protection of the rights and welfare of subjects.

(c) An IRB shall require documentation of informed consent or may waive documentation in accordance with § 46.117.

(d) An IRB shall notify investigators and the institution in writing of its decision to approve or disapprove the proposed research activity, or of modifications required to secure IRB approval of the research activity. If the IRB decides to disapprove a research activity, it shall include in its written notification a statement of the reasons for its decision and give the investigator an opportunity to respond in person or in writing.

(e) An IRB shall conduct continuing review of research covered by this policy at intervals appropriate to the degree of risk, but not less than once per year, and shall have authority to observe or have a third party observe the consent process and the research.

(Approved by the Office of Management and Budget under Control Number 0990-0260)

Official Citation:
[56 FR 28012, 28020, June 18, 1991, as amended at 70 FR 36328, June 23, 2005]
28 CFR Section 46.110: Expedited review procedures for certain kinds of research involving no more than minimal risk, and for minor changes in approved research.

(a) The Secretary, HHS, has established, and published as a Notice in the Federal Register, a list of categories of research that may be reviewed by the IRB through an expedited review procedure. The list will be amended, as appropriate after consultation with other departments and agencies, through periodic republication by the Secretary, HHS, in the Federal Register.

A copy of the list is available from the Office for Human Research Protections, HHS, or any successor office.

(b) An IRB may use the expedited review procedure to review either or both of the following:

(1) Some or all of the research appearing on the list and found by the reviewer(s) to involve no more than minimal risk,

(2) Minor changes in previously approved research during the period (of one year or less) for which approval is authorized.

Under an expedited review procedure, the review may be carried out by the IRB chairperson or by one or more experienced reviewers designated by the chairperson from among members of the IRB. In reviewing the research, the reviewers may exercise all of the authorities of the IRB except that the reviewers may not disapprove the research. A research activity may be disapproved only after review in accordance with the non-expedited procedure set forth in § 46.108(b).

(c) Each IRB which uses an expedited review procedure shall adopt a method for keeping all members advised of research proposals which have been approved under the procedure.

(d) The department or agency head may restrict, suspend, terminate, or choose not to authorize an institution's or IRB's use of the expedited review procedure.

Official Citation:
[56 FR 28012, 28020, June 18, 1991, as amended at 70 FR 36328, June 23, 2005]

28 CFR Section 46.111: Criteria for IRB approval of research.

(a) In order to approve research covered by this policy the IRB shall determine that all of the following requirements are satisfied:

---

Page 655
(1) Risks to subjects are minimized: (i) By using procedures which are consistent with sound research design and which do not unnecessarily expose subjects to risk, and (ii) whenever appropriate, by using procedures already being performed on the subjects for diagnostic or treatment purposes.

(2) Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result. In evaluating risks and benefits, the IRB should consider only those risks and benefits that may result from the research (as distinguished from risks and benefits of therapies subjects would receive even if not participating in the research). The IRB should not consider possible long-range effects of applying knowledge gained in the research (for example, the possible effects of the research on public policy) as among those research risks that fall within the purview of its responsibility.

(3) Selection of subjects is equitable. In making this assessment the IRB should take into account the purposes of the research and the setting in which the research will be conducted and should be particularly cognizant of the special problems of research involving vulnerable populations, such as children, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons.

(4) Informed consent will be sought from each prospective subject or the subject’s legally authorized representative, in accordance with, and to the extent required by § 46.116.

(5) Informed consent will be appropriately documented, in accordance with, and to the extent required by § 46.117.

(6) When appropriate, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects.

(7) When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

(b) When some or all of the subjects are likely to be vulnerable to coercion or undue influence, such as children, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons, additional safeguards have been included in the study to protect the rights and welfare of these subjects.
28 CFR Section 46.112: Review by institution.

Research covered by this policy that has been approved by an IRB may be subject to further appropriate review and approval or disapproval by officials of the institution. However, those officials may not approve the research if it has not been approved by an IRB.

28 CFR Section 46.113: Suspension or termination of IRB approval of research.

An IRB shall have authority to suspend or terminate approval of research that is not being conducted in accordance with the IRB’s requirements or that has been associated with unexpected serious harm to subjects. Any suspension or termination of approval shall include a statement of the reasons for the IRB’s action and shall be reported promptly to the investigator, appropriate institutional officials, and the department or agency head.

(Approved by the Office of Management and Budget under Control Number 0990-0260)

Official Citation:
[56 FR 28012, 28020, June 18, 1991, as amended at 70 FR 36328, June 23, 2005]

28 CFR Section 46.114: Cooperative research.

Cooperative research projects are those projects covered by this policy which involve more than one institution. In the conduct of cooperative research projects, each institution is responsible for safeguarding the rights and welfare of human subjects and for complying with this policy. With the approval of the department or agency head, an institution participating in a cooperative project may enter into a joint review arrangement, rely upon the review of another qualified IRB, or make similar arrangements for avoiding duplication of effort.

28 CFR Section 46.115: IRB records.

(a) An institution, or when appropriate an IRB, shall prepare and maintain adequate documentation of IRB activities, including the following:
(1) Copies of all research proposals reviewed, scientific evaluations, if any, that accompany the proposals, approved sample consent documents, progress reports submitted by investigators, and reports of injuries to subjects.

(2) Minutes of IRB meetings which shall be in sufficient detail to show attendance at the meetings; actions taken by the IRB; the vote on these actions including the number of members voting for, against, and abstaining; the basis for requiring changes in or disapproving research; and a written summary of the discussion of controverted issues and their resolution.

(3) Records of continuing review activities.

(4) Copies of all correspondence between the IRB and the investigators.

(5) A list of IRB members in the same detail as described is § 46.103(b)(3).

(6) Written procedures for the IRB in the same detail as described in § 46.103(b)(4) and § 46.103(b)(5).

(7) Statements of significant new findings provided to subjects, as required by § 46.116(b)(5).

(b) The records required by this policy shall be retained for at least 3 years, and records relating to research which is conducted shall be retained for at least 3 years after completion of the research. All records shall be accessible for inspection and copying by authorized representatives of the department or agency at reasonable times and in a reasonable manner.

(Approved by the Office of Management and Budget under Control Number 0990-0260)

Official Citation:
[56 FR 28012, 28020, June 18, 1991, as amended at 70 FR 36328, June 23, 2005]

28 CFR Section 46.116: General requirements for informed consent.

Except as provided elsewhere in this policy, no investigator may involve a human being as a subject in research covered by this policy unless the investigator has obtained the legally effective informed consent of the subject or the subject’s legally authorized representative. An investigator shall seek such consent only under circumstances that provide the prospective subject or the representative sufficient opportunity to consider whether or not to participate and that
minimize the possibility of coercion or undue influence. The information that is given to the subject or the representative shall be in language understandable to the subject or the representative. No informed consent, whether oral or written, may include any exculpatory language through which the subject or the representative is made to waive or appear to waive any of the subject's legal rights, or releases or appears to release the investigator, the sponsor, the institution or its agents from liability for negligence.

(a) Basic elements of informed consent. Except as provided in paragraph (c) or (d) of this section, in seeking informed consent the following information shall be provided to each subject:

(1) A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures which are experimental;

(2) A description of any reasonably foreseeable risks or discomforts to the subject;

(3) A description of any benefits to the subject or to others which may reasonably be expected from the research;

(4) A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject;

(5) A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained;

(6) For research involving more than minimal risk, an explanation as to whether any compensation and an explanation as to whether any medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained;

(7) An explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject; and

(8) A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.

(b) Additional elements of informed consent. When appropriate, one or more of the following elements of information shall also be provided to each subject:

---

Page 659
(1) A statement that the particular treatment or procedure may involve risks to the subject (or to the embryo or fetus, if the subject is or may become pregnant) which are currently unforeseeable;

(2) Anticipated circumstances under which the subject's participation may be terminated by the investigator without regard to the subject's consent;

(3) Any additional costs to the subject that may result from participation in the research;

(4) The consequences of a subject's decision to withdraw from the research and procedures for orderly termination of participation by the subject;

(5) A statement that significant new findings developed during the course of the research which may relate to the subject's willingness to continue participation will be provided to the subject; and

(6) The approximate number of subjects involved in the study.

(c) An IRB may approve a consent procedure which does not include, or which alters, some or all of the elements of informed consent set forth above, or waive the requirement to obtain informed consent provided the IRB finds and documents that:

(1) The research or demonstration project is to be conducted by or subject to the approval of state or local government officials and is designed to study, evaluate, or otherwise examine:

   (i) Public benefit of service programs;

   (ii) Procedures for obtaining benefits or services under those programs;

   (iii) Possible changes in or alternatives to those programs or procedures; or

   (iv) Possible changes in methods or levels of payment for benefits or services under those programs; and

(2) The research could not practicably be carried out without the waiver or alteration.

(d) An IRB may approve a consent procedure which does not include, or which alters, some or all of the elements of informed consent set forth in this section, or
waive the requirements to obtain informed consent provided the IRB finds and documents that:

(1) The research involves no more than minimal risk to the subjects;

(2) The waiver or alteration will not adversely affect the rights and welfare of the subjects;

(3) The research could not practicably be carried out without the waiver or alteration; and

(4) Whenever appropriate, the subjects will be provided with additional pertinent information after participation.

(e) The informed consent requirements in this policy are not intended to preempt any applicable federal, state, or local laws which require additional information to be disclosed in order for informed consent to be legally effective.

(f) Nothing in this policy is intended to limit the authority of a physician to provide emergency medical care, to the extent the physician is permitted to do so under applicable federal, state, or local law.

(Approved by the Office of Management and Budget under Control Number 0990-0260)

Official Citation:
[56 FR 28012, 28020, June 18, 1991, as amended at 70 FR 36328, June 23, 2005]

28 CFR Section 46.117: Documentation of informed consent.

(a) Except as provided in paragraph (c) of this section, informed consent shall be documented by the use of a written consent form approved by the IRB and signed by the subject or the subject's legally authorized representative. A copy shall be given to the person signing the form.

(b) Except as provided in paragraph (c) of this section, the consent form may be either of the following:

(1) A written consent document that embodies the elements of informed consent required by § 46.116. This form may be read to the subject or the subject's legally authorized representative, but in any event, the investigator shall give either the subject or the representative adequate opportunity to read it before it is signed; or
(2) A short form written consent document stating that the elements of informed consent required by § 46.116 have been presented orally to the subject or the subject’s legally authorized representative. When this method is used, there shall be a witness to the oral presentation. Also, the IRB shall approve a written summary of what is to be said to the subject or the representative. Only the short form itself is to be signed by the subject or the representative. However, the witness shall sign both the short form and a copy of the summary, and the person actually obtaining consent shall sign a copy of the summary. A copy of the summary shall be given to the subject or the representative, in addition to a copy of the short form.

(c) An IRB may waive the requirement for the investigator to obtain a signed consent form for some or all subjects if it finds either:

   (1) That the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality. Each subject will be asked whether the subject wants documentation linking the subject with the research, and the subject's wishes will govern; or

   (2) That the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.

In cases in which the documentation requirement is waived, the IRB may require the investigator to provide subjects with a written statement regarding the research.

(Approved by the Office of Management and Budget under Control Number 0990-0260)

Official Citation:
[56 FR 28012, 28020, June 18, 1991, as amended at 70 FR 36328, June 23, 2005]

28 CFR Section 46.118: Applications and proposals lacking definite plans for involvement of human subjects.

Certain types of applications for grants, cooperative agreements, or contracts are submitted to departments or agencies with the knowledge that subjects may be involved within the period of support, but definite plans would not normally be set forth in the application or proposal. These include activities such as institutional type grants when selection of specific projects is the institution's responsibility; research training grants in which the activities involving subjects
remain to be selected; and projects in which human subjects' involvement will depend upon completion of instruments, prior animal studies, or purification of compounds. These applications need not be reviewed by an IRB before an award may be made. However, except for research exempted or waived under § 46.101 (b) or (i), no human subjects may be involved in any project supported by these awards until the project has been reviewed and approved by the IRB, as provided in this policy, and certification submitted, by the institution, to the department or agency.

28 CFR Section 46.119: Research undertaken without the intention of involving human subjects.

In the event research is undertaken without the intention of involving human subjects, but it is later proposed to involve human subjects in the research, the research shall first be reviewed and approved by an IRB, as provided in this policy, a certification submitted, by the institution, to the department or agency, and final approval given to the proposed change by the department or agency.

28 CFR Section 46.120: Evaluation and disposition of applications and proposals for research to be conducted or supported by a Federal Department or Agency.

(a) The department or agency head will evaluate all applications and proposals involving human subjects submitted to the department or agency through such officers and employees of the department or agency and such experts and consultants as the department or agency head determines to be appropriate. This evaluation will take into consideration the risks to the subjects, the adequacy of protection against these risks, the potential benefits of the research to the subjects and others, and the importance of the knowledge gained or to be gained.

(b) On the basis of this evaluation, the department or agency head may approve or disapprove the application or proposal, or enter into negotiations to develop an approvable one.

Official Citation:

28 CFR Section 46.121: [Reserved]

Federal funds administered by a department or agency may not be expended for research involving human subjects unless the requirements of this policy have been satisfied.

28 CFR Section 46.123: Early termination of research support: Evaluation of applications and proposals.

(a) The department or agency head may require that department or agency support for any project be terminated or suspended in the manner prescribed in applicable program requirements, when the department or agency head finds an institution has materially failed to comply with the terms of this policy.

(b) In making decisions about supporting or approving applications or proposals covered by this policy the department or agency head may take into account, in addition to all other eligibility requirements and program criteria, factors such as whether the applicant has been subject to a termination or suspension under paragraph (a) of this section and whether the applicant or the person or persons who would direct or have directed the scientific and technical aspects of an activity has have, in the judgment of the department or agency head, materially failed to discharge responsibility for the protection of the rights and welfare of human subjects (whether or not the research was subject to federal regulation).

28 CFR Section 46.124: Conditions.

With respect to any research project or any class of research projects the department or agency head may impose additional conditions prior to or at the time of approval when in the judgment of the department or agency head additional conditions are necessary for the protection of human subjects.
28 CFR PART 47—RIGHT TO FINANCIAL PRIVACY ACT

- 28 CFR Section 47.1: Definitions.
- 28 CFR Section 47.2: Purpose.
- 28 CFR Section 47.3: Authorization.
- 28 CFR Section 47.4: Written request.
- 28 CFR Section 47.5: Certification.

Authority:

Source:
Order No. 822-79, 44 FR 14554, Mar. 13, 1979, unless otherwise noted.
28 CFR Section 47.1: Definitions.

The terms used in this part shall have the same meaning as similar terms used in the Right to Financial Privacy Act of 1978.

Departmental unit
means any office, division, board, bureau, or other component of the Department of Justice which is authorized to conduct law enforcement inquiries.

Act

28 CFR Section 47.2: Purpose.

The purpose of these regulations is to authorize Departmental units to request financial records from a financial institution pursuant to the formal written request procedure authorized by section 1108 of the Act, and to set forth the conditions under which such requests may be made.

28 CFR Section 47.3: Authorization.

Departmental units are authorized to request financial records of any customer from a financial institution pursuant to a formal written request under the Act only if:

(a) No administrative summons or subpoena authority reasonably appears to be available to the Departmental unit to obtain financial records for the purpose for which the records are sought;

(b) There is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry and will further that inquiry;

(c) The request is issued by a supervisory official of a rank designated by the head of the requesting Departmental unit. The officials so designated shall not delegate this authority to others;

(d) The request adheres to the requirements set forth in § 47.4; and

(e) The notice requirements set forth in section 1108(4) of the Act, or the requirements pertaining to delay of notice in section 1109 of the Act, are satisfied, except in situations (e.g., section 1113(g)) where no notice is required.
28 CFR Section 47.4: Written request.

(a) The formal written request shall be in the form of a letter or memorandum to an appropriate official of the financial institution from which financial records are requested. The request shall be signed by the issuing official, and shall set forth that official’s name, title, business address and business phone number. The request shall also contain the following:

(1) The identity of the customer or customers to whom the records pertain;

(2) A reasonable description of the records sought; and

(3) Such additional information as may be appropriate—e.g., the date on which the opportunity for the customer to challenge the formal written request will expire, the date on which the requesting Departmental unit expects to present a certificate of compliance with the applicable provisions of the Act, the name and title of the individual (if known) to whom disclosure is to be made.

(b) In cases where customer notice is delayed by court order, a copy of the court order shall be attached to the formal written request.

28 CFR Section 47.5: Certification.

Prior to obtaining the requested records pursuant to a formal written request, an official of a rank designated by the head of the requesting Departmental unit shall certify in writing to the financial institution that the Departmental unit has complied with the applicable provisions of the Act.
28 CFR PART 50—STATEMENTS OF POLICY

- 28 CFR Section 50.2: Release of information by personnel of the Department of Justice relating to criminal and civil proceedings.
- 28 CFR Section 50.3: Guidelines for the enforcement of title VI, Civil Rights Act of 1964.
- 28 CFR Section 50.5: Notification of Consular Officers upon the arrest of foreign nationals.
- 28 CFR Section 50.6: Antitrust Division business review procedure.
- 28 CFR Section 50.7: Consent judgments in actions to enjoin discharges of pollutants.
- 28 CFR Section 50.8: [Reserved]
- 28 CFR Section 50.9: Policy with regard to open judicial proceedings.
- 28 CFR Section 50.10: Policy with regard to the issuance of subpoenas to members of the news media, subpoenas for telephone toll records of members of the news media, and the interrogation, indictment, or arrest of, members of the news media.
- 28 CFR Section 50.12: Exchange of FBI identification records.
- 28 CFR Section 50.15: Representation of Federal officials and employees by Department of Justice attorneys or by private counsel furnished by the Department in civil, criminal, and congressional proceedings in which Federal employees are sued, subpoenaed, or charged in their individual capacities.
- 28 CFR Section 50.16: Representation of Federal employees by private counsel at Federal expense.
- 28 CFR Section 50.17: Ex parte communications in informal rulemaking proceedings.
- 28 CFR Section 50.18: [Reserved]
- 28 CFR Section 50.19: Procedures to be followed by government attorneys prior to filing recusal or disqualification motions.
- 28 CFR Section 50.20: Participation by the United States in court-annexed arbitration.
- 28 CFR Section 50.21: Procedures governing the destruction of contraband drug evidence in the custody of Federal law enforcement authorities.
- 28 CFR Section 50.22: Young American Medals Program.
- 28 CFR Section 50.23: Policy against entering into final settlement agreements or consent decree that are subject to confidentiality provisions and against seeking or concurring in the sealing of such documents.
- 28 CFR Section 50.24: Annuity broker minimum qualifications.

Authority:
28 CFR Section 50.2: Release of information by personnel of the Department of Justice relating to criminal and civil proceedings.

(a) General.
(1) The availability to news media of information in criminal and civil cases is a matter which has become increasingly a subject of concern in the administration of justice. The purpose of this statement is to formulate specific guidelines for the release of such information by personnel of the Department of Justice.

(2) While the release of information for the purpose of influencing a trial is, of course, always improper, there are valid reasons for making available to the public information about the administration of the law. The task of striking a fair balance between the protection of individuals accused of crime or involved in civil proceedings with the Government and public understandings of the problems of controlling crime and administering government depends largely on the exercise of sound judgment by those responsible for administering the law and by representatives of the press and other media.

(3) Inasmuch as the Department of Justice has generally fulfilled its responsibilities with awareness and understanding of the competing needs in this area, this statement, to a considerable extent, reflects and formalizes the standards to which representatives of the Department have adhered in the past. Nonetheless, it will be helpful in ensuring uniformity of practice to set forth the following guidelines for all personnel of the Department of Justice.

(4) Because of the difficulty and importance of the questions they raise, it is felt that some portions of the matters covered by this statement, such as the authorization to make available Federal conviction records and a description of items seized at the time of arrest, should be the subject of continuing review and consideration by the Department on the basis of experience and suggestions from those within and outside the Department.

(b) Guidelines to criminal actions.
(1) These guidelines shall apply to the release of information to news media from the time a person is the subject of a criminal investigation until any proceeding resulting from such an investigation has been terminated by trial or otherwise.

(2) At no time shall personnel of the Department of Justice furnish any statement or information for the purpose of influencing the outcome of a defendant’s trial, nor shall personnel of the Department furnish any statement or information, which could reasonably be expected to be disseminated by means of public communication, if such a statement or information may reasonably be expected to influence the outcome of a pending or future trial.
(3) Personnel of the Department of Justice, subject to specific limitations imposed by law or court rule or order, may make public the following information:

(i) The defendant's name, age, residence, employment, marital status, and similar background information.

(ii) The substance or text of the charge, such as a complaint, indictment, or information.

(iii) The identity of the investigating and/or arresting agency and the length or scope of an investigation.

(iv) The circumstances immediately surrounding an arrest, including the time and place of arrest, resistance, pursuit, possession and use of weapons, and a description of physical items seized at the time of arrest.

Disclosures should include only incontrovertible, factual matters, and should not include subjective observations. In addition, where background information or information relating to the circumstances of an arrest or investigation would be highly prejudicial or where the release thereof would serve no law enforcement function, such information should not be made public.

(4) Personnel of the Department shall not disseminate any information concerning a defendant's prior criminal record.

(5) Because of the particular danger of prejudice resulting from statements in the period approaching and during trial, they ought strenuously to be avoided during that period. Any such statement or release shall be made only on the infrequent occasion when circumstances absolutely demand a disclosure of information and shall include only information which is clearly not prejudicial.

(6) The release of certain types of information generally tends to create dangers of prejudice without serving a significant law enforcement function. Therefore, personnel of the Department should refrain from making available the following:

(i) Observations about a defendant's character.

(ii) Statements, admissions, confessions, or alibis attributable to a defendant, or the refusal or failure of the accused to make a statement.

(iii) Reference to investigative procedures such as fingerprints, polygraph examinations, ballistic tests, or laboratory tests, or to the refusal by the defendant to submit to such tests or examinations.
(iv) Statements concerning the identity, testimony, or credibility of prospective witnesses.

(v) Statements concerning evidence or argument in the case, whether or not it is anticipated that such evidence or argument will be used at trial.

(vi) Any opinion as to the accused’s guilt, or the possibility of a plea of guilty to the offense charged, or the possibility of a plea to a lesser offense.

(7) Personnel of the Department of Justice should take no action to encourage or assist news media in photographing or televising a defendant or accused person being held or transported in Federal custody. Departmental representatives should not make available photographs of a defendant unless a law enforcement function is served thereby.

(8) This statement of policy is not intended to restrict the release of information concerning a defendant who is a fugitive from justice.

(9) Since the purpose of this statement is to set forth generally applicable guidelines, there will, of course, be situations in which it will limit the release of information which would not be prejudicial under the particular circumstances. If a representative of the Department believes that in the interest of the fair administration of justice and the law enforcement process information beyond these guidelines should be released, in a particular case, he shall request the permission of the Attorney General or the Deputy Attorney General to do so.

(c) Guidelines to civil actions. Personnel of the Department of Justice associated with a civil action shall not during its investigation or litigation make or participate in making an extrajudicial statement, other than a quotation from or reference to public records, which a reasonable person would expect to be disseminated by means of public communication if there is a reasonable likelihood that such dissemination will interfere with a fair trial and which relates to:

(1) Evidence regarding the occurrence or transaction involved.

(2) The character, credibility, or criminal records of a party, witness, or prospective witness.

(3) The performance or results of any examinations or tests or the refusal or failure of a party to submit to such.
(4) An opinion as to the merits of the claims or defenses of a party, except as required by law or administrative rule.

(5) Any other matter reasonably likely to interfere with a fair trial of the action.

**Official Citation:**

---

28 CFR Section 50.3: Guidelines for the enforcement of title VI, Civil Rights Act of 1964.

(a) Where the heads of agencies having responsibilities under title VI of the Civil Rights Act of 1964 conclude there is noncompliance with regulations issued under that title, several alternative courses of action are open. In each case, the objective should be to secure prompt and full compliance so that needed Federal assistance may commence or continue.

(b) Primary responsibility for prompt and vigorous enforcement of title VI rests with the head of each department and agency administering programs of Federal financial assistance. Title VI itself and relevant Presidential directives preserve in each agency the authority and the duty to select, from among the available sanctions, the methods best designed to secure compliance in individual cases. The decision to terminate or refuse assistance is to be made by the agency head or his designated representative.

(c) This statement is intended to provide procedural guidance to the responsible department and agency officials in exercising their statutory discretion and in selecting, for each noncompliance situation, a course of action that fully conforms to the letter and spirit of section 602 of the Act and to the implementing regulations promulgated thereunder.

I. Alternative Courses of Action
   a. ultimate sanctions
The ultimate sanctions under title VI are the refusal to grant an application for assistance and the termination of assistance being rendered. Before these sanctions may be invoked, the Act requires completion of the procedures called for by section 602. That section require the department or agency concerned (1) to determine that compliance cannot be secured by voluntary means, (2) to consider alternative courses of action consistent with achievement of the objectives of the statutes authorizing the particular financial assistance, (3) to afford the applicant an opportunity for a hearing, and (4) to complete the other procedural steps...
outlined in section 602, including notification to the appropriate committees of the Congress.

In some instances, as outlined below, it is legally permissible temporarily to defer action on an application for assistance, pending initiation and completion of section 602 procedures—including attempts to secure voluntary compliance with title VI. Normally, this course of action is appropriate only with respect to applications for noncontinuing assistance or initial applications for programs of continuing assistance. It is not available where Federal financial assistance is due and payable pursuant to a previously approved application.

Whenever action upon an application is deferred pending the outcome of a hearing and subsequent section 602 procedures, the efforts to secure voluntary compliance and the hearing and such subsequent procedures, if found necessary, should be conducted without delay and completed as soon as possible.

b. available alternatives

1. Court Enforcement

Compliance with the nondiscrimination mandate of title VI may often be obtained more promptly by appropriate court action than by hearings and termination of assistance. Possibilities of judicial enforcement include(1) a suit to obtain specific enforcement of assurances, covenants running with federally provided property, statements or compliance or desegregation plans filed pursuant to agency regulations, (2) a suit to enforce compliance with other titles of the 1964 Act, other Civil Rights Acts, or constitutional or statutory provisions requiring nondiscrimination, and (3) initiation of, or intervention or other participation in, a suit for other relief designed to secure compliance.

The possibility of court enforcement should not be rejected without consulting the Department of Justice. Once litigation has been begun, the affected agency should consult with the Department of Justice before taking any further action with respect to the noncomplying party.

2. Administrative Action

A number of effective alternative courses not involving litigation may also be available in many cases. These possibilities include(1) consulting with or seeking assistance from other Federal agencies (such as the Contract Compliance Division of the Department of Labor) having authority to enforce nondiscrimination requirements; (2) consulting with or seeking assistance from State or local agencies having such authority; (3) bypassing a recalcitrant central agency applicant in order to obtain assurances from, or to grant assistance to complying local agencies; and (4) bypassing all recalcitrant non-Federal agencies and providing assistance directly to the complying ultimate beneficiaries. The possibility of utilizing such administrative alternatives should be considered at all stages of enforcement and used as appropriate or feasible.
c. inducing voluntary compliance
Title VI requires that a concerted effort be made to persuade any noncomplying applicant or recipient voluntarily to comply with title VI. Efforts to secure voluntary compliance should be undertaken at the outset in every noncompliance situation and should be pursued through each stage of enforcement action. Similarly, where an applicant fails to file an adequate assurance or apparently breaches its terms, notice should be promptly given of the nature of the noncompliance problem and of the possible consequences thereof, and an immediate effort made to secure voluntary compliance.

II. Procedures
a. new applications

The following procedures are designed to apply in cases of noncompliance involving applications for one-time or noncontinuing assistance and initial applications for new or existing programs of continuing assistance.

Source:
1. Where the Requisite Assurance Has Not Been Filed or Is Inadequate on Its Face.

Where the assurance, statement of compliance or plan of desegregation required by agency regulations has not been filed or where, in the judgment of the head of the agency in question, the filed assurance fails on its face to satisfy the regulations, the agency head should defer action on the application pending prompt initiation and completion of section 602 procedures. The applicant should be notified immediately and attempts made to secure voluntary compliance. If such efforts fail, the applicant should promptly be offered a hearing for the purpose of determining whether an adequate assurance has in fact been filed.

If it is found that an adequate assurance has not been filed, and if administrative alternatives are ineffective or inappropriate, and court enforcement is not feasible, section 602 procedures may be completed and assistance finally refused.

Source:
2. Where it Appears that the Field Assurance Is Untrue or Is Not Being Honored.

Where an otherwise adequate assurance, statement of compliance, or plan has been filed in connection with an application for assistance, but prior to
completion of action on the application the head of the agency in question has reasonable grounds, based on a substantiated complaint, the agency's own investigation, or otherwise, to believe that the representations as to compliance are in some material respect untrue or are not being honored, the agency head may defer action on the application pending prompt initiation and completion of section 602 procedures. The applicant should be notified immediately and attempts made to secure voluntary compliance. If such efforts fail and court enforcement is determined to be ineffective or inadequate, a hearing should be promptly initiated to determine whether, in fact, there is noncompliance.

If noncompliance is found, and if administrative alternatives are ineffective or inappropriate and court enforcement is still not feasible, section 602 procedures may be completed and assistance finally refused.

The above-described deferral and related compliance procedures would normally be appropriate in cases of an application for noncontinuing assistance. In the case of an initial application for a new or existing program of continuing assistance, deferral would often be less appropriate because of the opportunity to secure full compliance during the life of the assistance program. In those cases in which the agency does not defer action on the application, the applicant should be given prompt notice of the asserted noncompliance; funds should be paid out for short periods only, with no long-term commitment of assistance given; and the applicant advised that acceptance of the funds carries an enforceable obligation of nondiscrimination and the risk of invocation of severe sanctions, if noncompliance in fact is found.

b. requests for continuation or renewal of assistance
The following procedures are designed to apply in cases of noncompliance involving all submissions seeking continuation or renewal under programs of continuing assistance.

In cases in which commitments for Federal financial assistance have been made prior to the effective date of title VI regulations and funds have not been fully disbursed, or in which there is provision for future periodic payments to continue the program or activity for which a present recipient has previously applied and qualified, or in which assistance is given without formal application pursuant to statutory direction or authorization, the responsible agency may nonetheless require an assurance, statement of compliance, or plan in connection with disbursement or further funds. However, once a particular program grant or loan has been made or an application for a certain type of assistance for a specific or indefinite period has been approved, no funds due and payable pursuant to that grant, loan, or application, may normally be deferred or withheld without first completing the procedures prescribed in section 602.
Accordingly, where the assurance, statement of compliance, or plan required by agency regulations has not been filed or where, in the judgment of the head of the agency in question, the filed assurance fails on its face to satisfy the regulations, or there is reasonable cause to believe it untrue or not being honored, the agency head should, if efforts to secure voluntary compliance are unsuccessful, promptly institute a hearing to determine whether an adequate assurance has in fact been filed, or whether, in fact, there is noncompliance, as the case may be. There should ordinarily be no deferral of action on the submission or withholding of funds in this class of cases, although the limitation of the payout of funds to short periods may appropriately be ordered. If noncompliance is found, and if administrative alternatives are ineffective or inappropriate and court enforcement is not feasible, section 602 procedures may be completed and assistance terminated.

c. short-term programs
Special procedures may sometimes be required where there is noncompliance with title VI regulations in connection with a program of such short total duration that all assistance funds will have to be paid out before the agency's usual administrative procedures can be completed and where deferral in accordance with these guidelines would be tantamount to a final refusal to grant assistance.

In such a case, the agency head may, although otherwise following these guidelines, suspend normal agency procedures and institute expedited administrative proceedings to determine whether the regulations have been violated. He should simultaneously refer the matter to the Department of Justice for consideration of possible court enforcement, including interim injunctive relief. Deferral of action on an application is appropriate, in accordance with these guidelines, for a reasonable period of time, provided such action is consistent with achievement of the objectives of the statute authorizing the financial assistance in connection with the action taken. As in other cases, where noncompliance is found in the hearing proceeding, and if administrative alternatives are ineffective or inappropriate and court enforcement is not feasible, section 602 procedures may be completed and assistance finally refused.

III. Procedures in Cases of Subgrantees
In situations in which applications for Federal assistance are approved by some agency other than the Federal granting agency, the same rules and procedures would apply. Thus, the Federal Agency should instruct the approving agency—typically a State agency—to defer approval or refuse to grant funds, in individual cases in which such action would be taken by the original granting agency itself under the above procedures. Provision should be made for appropriate notice of such action to the Federal agency which retains responsibility for compliance with section 602 procedures.

IV. Exceptional Circumstances
The Attorney General should be consulted in individual cases in which the head of an agency believes that the objectives of title VI will be best achieved by proceeding other than as provided in these guidelines.

V. Coordination

While primary responsibility for enforcement of title VI rests directly with the head of each agency, in order to assure coordination of title VI enforcement and consistency among agencies, the Department of Justice should be notified in advance of applications on which action is to be deferred, hearings to be scheduled, and refusals and terminations of assistance or other enforcement actions or procedures to be undertaken. The Department also should be kept advised of the progress and results of hearings and other enforcement actions.

Official Citation:
[31 FR 5292, Apr. 2, 1966]

28 CFR Section 50.5: Notification of Consular Officers upon the arrest of foreign nationals.

(a) This statement is designed to establish a uniform procedure for consular notification where nationals of foreign countries are arrested by officers of this Department on charges of criminal violations. It conforms to practice under international law and in particular implements obligations undertaken by the United States pursuant to treaties with respect to the arrest and detention of foreign nationals. Some of the treaties oblige the United States to notify the consular officer only upon the demand or request of the arrested foreign national. On the other hand, some of the treaties require notifying the consul of the arrest of a foreign national whether or not the arrested person requests such notification.

(1) In every case in which a foreign national is arrested the arresting officer shall inform the foreign national that his consul will be advised of his arrest unless he does not wish such notification to be given. If the foreign national does not wish to have his consul notified, the arresting officer shall also inform him that in the event there is a treaty in force between the United States and his country which requires such notification, his consul must be notified regardless of his wishes and, if such is the case, he will be advised of such notification by the U.S. Attorney.

(2) In all cases (including those where the foreign national has stated that he does not wish his consul to be notified) the local office of the Federal Bureau of Investigation or the local Marshal’s office, as the case may be, shall inform the
nearest U.S. Attorney of the arrest and of the arrested person’s wishes regarding consular notification.

(3) The U.S. Attorney shall then notify the appropriate consul except where he has been informed that the foreign national does not desire such notification to be made. However, if there is a treaty provision in effect which requires notification of consul, without reference to a demand or request of the arrested national, the consul shall be notified even if the arrested person has asked that he not be notified. In such case, the U.S. Attorney shall advise the foreign national that his consul has been notified and inform him that notification was necessary because of the treaty obligation.

(b) The procedure prescribed by this statement shall not apply to cases involving arrests made by the Immigration and Naturalization Service in administrative expulsion or exclusion proceedings, since that Service has heretofore established procedures for the direct notification of the appropriate consular officer upon such arrest. With respect to arrests made by the Service for violations of the criminal provisions of the immigration laws, the U.S. Marshal, upon delivery of the foreign national into his custody, shall be responsible for informing the U.S. Attorney of the arrest in accordance with numbered paragraph 2 of this statement.

**Official Citation:**

---

28 CFR Section 50.6: Antitrust Division business review procedure.

Although the Department of Justice is not authorized to give advisory opinions to private parties, for several decades the Antitrust Division has been willing in certain circumstances to review proposed business conduct and state its enforcement intentions. This originated with a “railroad release” procedure under which the Division would forego the initiation of criminal antitrust proceedings. The procedure was subsequently expanded to encompass a “merger clearance” procedure under which the Division would state its present enforcement intention with respect to a merger or acquisition; and the Department issued a written statement entitled “Business Review Procedure.” That statement has been revised several times.

1. A request for a business review letter must be submitted in writing to the Assistant Attorney General, Antitrust Division, Department of Justice, Washington, DC 20530.
2. The Division will consider only requests with respect to proposed business conduct, which may involve either domestic or foreign commerce.

3. The Division may, in its discretion, refuse to consider a request.

4. A business review letter shall have no application to any party which does not join in the request therefor.

5. The requesting parties are under an affirmative obligation to make full and true disclosure with respect to the business conduct for which review is requested. Each request must be accompanied by all relevant data including background information, complete copies of all operative documents and detailed statements of all collateral oral understandings, if any. All parties requesting the review letter must provide the Division with whatever additional information or documents the Division may thereafter request in order to review the matter. Such additional information, if furnished orally, shall be promptly confirmed in writing. In connection with any request for review the Division will also conduct whatever independent investigation it believes is appropriate.

6. No oral clearance, release or other statement purporting to bind the enforcement discretion of the Division may be given. The requesting party may rely upon only a written business review letter signed by the Assistant Attorney General in charge of the Antitrust Division or his delegate.

7. (a) If the business conduct for which review is requested is subject to approval by a regulatory agency, a review request may be considered before agency approval has been obtained only where it appears that exceptional and unnecessary burdens might otherwise be imposed on the party or parties requesting review, or where the agency specifically requests that a party or parties request review. However, any business review letter issued in these circumstances will state only the Department's present enforcement intentions under the antitrust laws. It shall in no way be taken to indicate the Department's views on the legal or factual issues that may be raised before the regulatory agency, or in an appeal from the regulatory agency's decision. In particular, the issuance of such a letter is not to be represented to mean that the Division believes that there are no anticompetitive consequences warranting agency consideration.

   (b) The submission of a request for a business review, or its pendency, shall in no way alter any responsibility of any party to comply with the Premerger Notification provisions of the Antitrust Improvements Act of 1976, 15 U.S.C. 18A, and the regulations promulgated thereunder, 16 CFR, part 801.

8. After review of a request submitted hereunder the Division may: state its present enforcement intention with respect to the proposed business conduct;
decline to pass on the request; or take such other position or action as it considers appropriate.

9. A business review letter states only the enforcement intention of the Division as of the date of the letter, and the Division remains completely free to bring whatever action or proceeding it subsequently comes to believe is required by the public interest. As to a stated present intention not to bring an action, however, the Division has never exercised its right to bring a criminal action where there has been full and true disclosure at the time of presenting the request.

10. (a) Simultaneously upon notifying the requesting party of an action described in paragraph 8, the business review request, and the Division's letter in response shall be indexed and placed in a file available to the public upon request.

(b) On that date or within thirty days after the date upon which the Division takes any action as described in paragraph 8, the information supplied to support the business review request and any other information supplied by the requesting party in connection with the transaction that is the subject of the business review request, shall be indexed and placed in a file with the request and the Division's letter, available to the public upon request. This file shall remain open for one year, after which time it shall be closed and the documents either returned to the requesting party or otherwise disposed of, at the discretion of the Antitrust Division.

(c) Prior to the time the information described in subparagraphs (a) and (b) is indexed and made publicly available in accordance with the terms of that subparagraph, the requesting party may ask the Division to delay making public some or all of such information. However the requesting party must: (1) Specify precisely the documents or parts thereof that he asks not be made public; (2) state the minimum period of time during which nondisclosure is considered necessary; and (3) justify the request for non-disclosure, both as to content and time, by showing good cause therefor, including a showing that disclosure would have a detrimental effect upon the requesting party's operations or relationships with actual or potential customers, employees, suppliers (including suppliers of credit), stockholders, or competitors. The Department of Justice, in its discretion, shall make the final determination as to whether good cause for non-disclosure has been shown.

(d) Nothing contained in subparagraphs (a), (b) and (c) shall limit the Division's right, in its discretion, to issue a press release describing generally the identity of the requesting party or parties and the nature of action taken by the Division upon the request.
(e) This paragraph reflects a policy determination by the Justice Department and is subject to any limitations on public disclosure arising from statutory restrictions, Executive Order, or the national interest.

11. Any requesting party may withdraw a request for review at any time. The Division remains free, however, to submit such comments to such requesting party as it deems appropriate. Failure to take action after receipt of documents or information whether submitted pursuant to this procedure or otherwise, does not in any way limit or stop the Division from taking such action at such time thereafter as it deems appropriate. The Division reserves the right to retain documents submitted to it under this procedure or otherwise and to use them for all governmental purposes.

**Official Citation:**
[42 FR 11831, Mar. 1, 1977]

**28 CFR Section 50.7:** Consent judgments in actions to enjoin discharges of pollutants.

(a) It is hereby established as the policy of the Department of Justice to consent to a proposed judgment in an action to enjoin discharges of pollutants into the environment only after or on condition that an opportunity is afforded persons (natural or corporate) who are not named as parties to the action to comment on the proposed judgment prior to its entry by the court.

(b) To effectuate this policy, each proposed judgment which is within the scope of paragraph (a) of this section shall be lodged with the court as early as feasible but at least 30 days before the judgment is entered by the court. Prior to entry of the judgment, or some earlier specified date, the Department of Justice will receive and consider, and file with the court, any written comments, views or allegations relating to the proposed judgment. The Department shall reserve the right (1) to withdraw or withhold its consent to the proposed judgment if the comments, views and allegations concerning the judgment disclose facts or considerations which indicate that the proposed judgment is inappropriate, improper or inadequate and (2) to oppose an attempt by any person to intervene in the action.

(c) The Assistant Attorney General in charge of the Land and Natural Resources Division may establish procedures for implementing this policy. Where it is clear that the public interest in the policy hereby established is not compromised, the Assistant Attorney General may permit an exception to this policy in a specific case where extraordinary circumstances require a period shorter than 30 days or a procedure other than stated herein.
28 CFR Section 50.8: [Reserved]

28 CFR Section 50.9: Policy with regard to open judicial proceedings.

Because of the vital public interest in open judicial proceedings, the Government has a general overriding affirmative duty to oppose their closure. There is, moreover, a strong presumption against closing proceedings or portions thereof, and the Department of Justice foresees very few cases in which closure would be warranted. The Government should take a position on any motion to close a judicial proceeding, and should ordinarily oppose closure; it should move for or consent to closed proceedings only when closure is plainly essential to the interests of justice. In furtherance of the Department's concern for the right of the public to attend judicial proceedings and the Department's obligation to the fair administration of justice, the following guidelines shall be adhered to by all attorneys for the United States.

(a) These guidelines apply to all federal trials, pre- and post-trial evidentiary proceedings, arraignments, bond hearings, plea proceedings, sentencing proceedings, or portions thereof, except as indicated in paragraph (e) of this section.

(b) A Government attorney has a compelling duty to protect the societal interest in open proceedings.

(c) A Government attorney shall not move for or consent to closure of a proceeding covered by these guidelines unless:

(1) No reasonable alternative exists for protecting the interests at stake;

(2) Closure is clearly likely to prevent the harm sought to be avoided;

(3) The degree of closure is minimized to the greatest extent possible;

(4) The public is given adequate notice of the proposed closure; and, in addition, the motion for closure is made on the record, except where the disclosure of the details of the motion papers would clearly defeat the reason for closure specified under paragraph (c)(6) of this section;

________________________________________________________

Page 682
(5) Transcripts of the closed proceedings will be unsealed as soon as the interests requiring closure no longer obtain; and

(6) Failure to close the proceedings will produce;

   (i) A substantial likelihood of denial of the right of any person to a fair trial; or

   (ii) A substantial likelihood of imminent danger to the safety of parties, witnesses, or other persons; or

   (iii) A substantial likelihood that ongoing investigations will be seriously jeopardized.

(d) A government attorney shall not move for or consent to the closure of any proceeding, civil or criminal, except with the express authorization of:

   (1) The Deputy Attorney General, or,

   (2) The Associate Attorney General, if the Division seeking authorization is under the supervision of the Associate Attorney General.

(e) These guidelines do not apply to:

   (1) The closure of part of a judicial proceeding where necessary to protect national security information or classified documents; or

   (2) In camera inspection, consideration or sealing of documents, including documents provided to the Government under a promise of confidentiality, where permitted by statute, rule of evidence or privilege; or

   (3) Grand jury proceedings or proceedings ancillary thereto; or

   (4) Conferences traditionally held at the bench or in chambers during the course of an open proceeding; or

   (5) The closure of judicial proceedings pursuant to 18 U.S.C. 3509 (d) and (e) for the protection of child victims or child witnesses.

(f) Because of the vital public interest in open judicial proceedings, the records of any proceeding closed pursuant to this section, and still sealed 60 days after termination of the proceeding, shall be reviewed to determine if the reasons for closure are still applicable. If they are not, an appropriate motion will be made to have the records unsealed. If the reasons for closure are still applicable after 60 days, this review is to be repeated every 60 days until such time as the records are
unsealed. Compliance with this section will be monitored by the Criminal Division.

(g) The principles set forth in this section are intended to provide guidance to attorneys for the Government and are not intended to create or recognize any legally enfor
cbly right in any person.

**Official Citation:**

28 CFR Section 50.10: Policy with regard to the issuance of subpoenas to members of the news media, subpoenas for telephone toll records of members of the news media, and the interrogation, indictment, or arrest of, members of the news media.

Because freedom of the press can be no broader than the freedom of reporters to investigate and report the news, the prosecutorial power of the government should not be used in such a way that it impairs a reporter's responsibility to cover as broadly as possible controversial public issues. This policy statement is thus intended to provide protection for the news media from forms of compulsory process, whether civil or criminal, which might impair the news gathering function. In balancing the concern that the Department of Justice has for the work of the news media and the Department's obligation to the fair administration of justice, the following guidelines shall be adhered to by all members of the Department in all cases:

(a) In determining whether to request issuance of a subpoena to a member of the news media, or for telephone toll records of any member of the news media, the approach in every case must be to strike the proper balance between the public's interest in the free dissemination of ideas and information and the public's interest in effective law enforcement and the fair administration of justice.

(b) All reasonable attempts should be made to obtain information from alternative sources before considering issuing a subpoena to a member of the news media, and similarly all reasonable alternative investigative steps should be taken before considering issuing a subpoena for telephone toll records of any member of the news media.

(c) Negotiations with the media shall be pursued in all cases in which a subpoena to a member of the news media is contemplated. These negotiations should attempt to accommodate the interests of the trial or grand jury with the interests of the media. Where the nature of the investigation permits, the government
should make clear what its needs are in a particular case as well as its willingness to respond to particular problems of the media.

(d) Negotiations with the affected member of the news media shall be pursued in all cases in which a subpoena for the telephone toll records of any member of the news media is contemplated where the responsible Assistant Attorney General determines that such negotiations would not pose a substantial threat to the integrity of the investigation in connection with which the records are sought. Such determination shall be reviewed by the Attorney General when considering a subpoena authorized under paragraph (e) of this section.

(e) No subpoena may be issued to any member of the news media or for the telephone toll records of any member of the news media without the express authorization of the Attorney General: Provided that, if a member of the news media with whom negotiations are conducted under paragraph (c) of this section expressly agrees to provide the material sought, and if that material has already been published or broadcast, the United States Attorney or the responsible Assistant Attorney General, after having been personally satisfied that the requirements of this section have been met, may authorize issuance of the subpoena and shall thereafter submit to the Office of Public Affairs a report detailing the circumstances surrounding the issuance of the subpoena.

(f) In requesting the Attorney General’s authorization for a subpoena to a member of the news media, the following principles will apply:

1. In criminal cases, there should be reasonable grounds to believe, based on information obtained from nonmedia sources, that a crime has occurred, and that the information sought is essential to a successful investigation—particularly with reference to directly establishing guilt or innocence. The subpoena should not be used to obtain peripheral, nonessential, or speculative information.

2. In civil cases there should be reasonable grounds, based on nonmedia sources, to believe that the information sought is essential to the successful completion of the litigation in a case of substantial importance. The subpoena should not be used to obtain peripheral, nonessential, or speculative information.

3. The government should have unsuccessfully attempted to obtain the information from alternative nonmedia sources.

4. The use of subpoenas to members of the news media should, except under exigent circumstances, be limited to the verification of published information and to such surrounding circumstances as relate to the accuracy of the published information.
(5) Even subpoena authorization requests for publicly disclosed information should be treated with care to avoid claims of harassment.

(6) Subpoenas should, wherever possible, be directed at material information regarding a limited subject matter, should cover a reasonably limited period of time, and should avoid requiring production of a large volume of unpublished material. They should give reasonable and timely notice of the demand for documents.

(g) In requesting the Attorney General's authorization for a subpoena for the telephone toll records of members of the news media, the following principles will apply:

(1) There should be reasonable ground to believe that a crime has been committed and that the information sought is essential to the successful investigation of that crime. The subpoena should be as narrowly drawn as possible; it should be directed at relevant information regarding a limited subject matter and should cover a reasonably limited time period. In addition, prior to seeking the Attorney General's authorization, the government should have pursued all reasonable alternative investigation steps as required by paragraph (b) of this section.

(2) When there have been negotiations with a member of the news media whose telephone toll records are to be subpoenaed, the member shall be given reasonable and timely notice of the determination of the Attorney General to authorize the subpoena and that the government intends to issue it.

(3) When the telephone toll records of a member of the news media have been subpoenaed without the notice provided for in paragraph (e)(2) of this section, notification of the subpoena shall be given the member of the news media as soon thereafter as it is determined that such notification will no longer pose a clear and substantial threat to the integrity of the investigation. In any event, such notification shall occur within 45 days of any return made pursuant to the subpoena, except that the responsible Assistant Attorney General may authorize delay of notification for no more than an additional 45 days.

(4) Any information obtained as a result of a subpoena issued for telephone toll records shall be closely held so as to prevent disclosure of the information to unauthorized persons or for improper purposes.

(h) No member of the Department shall subject a member of the news media to questioning as to any offense which he is suspected of having committed in the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of his official duties as a member of the news media,
without the express authority of the Attorney General: Provided, however, that
where exigent circumstances preclude prior approval, the requirements of
paragraph (l) of this section shall be observed.

(i) A member of the Department shall secure the express authority
of the Attorney General before a warrant for an arrest is sought, and whenever
possible before an arrest not requiring a warrant, of a member of the news media
for any offense which he is suspected of having committed in the course of, or
arising out of, the coverage or investigation of a news story, or while engaged in
the performance of his official duties as a member of the news media.

(j) No member of the Department shall present information to a grand jury
seeking a bill of indictment, or file an information, against a member of the news
media for any offense which he is suspected of having committed in the course of, or
arising out of, the coverage or investigation of a news story, or while engaged in
the performance of his official duties as a member of the news media, without
the express authority of the Attorney General.

(k) In requesting the Attorney General's authorization to question, to arrest or to
seek an arrest warrant for, or to present information to a grand jury seeking a bill
of indictment or to file an information against, a member of the news media for
an offense which he is suspected of having committed during the course of, or
arising out of, the coverage or investigation of a news story, or committed while
engaged in the performance of his official duties as a member of the news media,
a member of the Department shall state all facts necessary for determination of
the issues by the Attorney General. A copy of the request shall be sent to the
Director of Public Affairs.

(l) When an arrest or questioning of a member of the news media is necessary
before prior authorization of the Attorney General can be obtained, notification
of the arrest or questioning, the circumstances demonstrating that an exception
to the requirement of prior authorization existed, and a statement containing the
information that would have been given in requesting prior authorization, shall
be communicated immediately to the Attorney General and to the Director of
Public Affairs.

(m) In light of the intent of this section to protect freedom of the press, news
gathering functions, and news media sources, this policy statement does not
apply to demands for purely commercial or financial information unrelated to the
news gathering function.

(n) Failure to obtain the prior approval of the Attorney General may constitute
grounds for an administrative reprimand or other appropriate disciplinary
action. The principles set forth in this section are not intended to create or
recognize any legally enforceable right in any person.
Official Citation:
[Order No. 916-80, 45 FR 76436, Nov. 19, 1980]

28 CFR Section 50.12: Exchange of FBI identification records.

(a) The Federal Bureau of Investigation, hereinafter referred to as the FBI, is authorized to expend funds for the exchange of identification records with officials of federally chartered or insured banking institutions to promote or maintain the security of those institutions and, if authorized by state statute and approved by the Director of the FBI, acting on behalf of the Attorney General, with officials of state and local governments for purposes of employment and licensing, pursuant to section 201 of Public Law 92-544, 86 Stat. 1115. Also, pursuant to 15 U.S.C. 78q, 7 U.S.C. 21 (b)(4)(E), and 42 U.S.C. 2169, respectively, such records can be exchanged with certain segments of the securities industry, with registered futures associations, and with nuclear power plants. The records also may be exchanged in other instances as authorized by federal law.

(b) The FBI Director is authorized by 28 CFR 0.85(j) to approve procedures relating to the exchange of identification records. Under this authority, effective September 6, 1990, the FBI Criminal Justice Information Services (CJIS) Division has made all data on identification records available for such purposes. Records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Officials at the governmental institutions and other entities authorized to submit fingerprints and receive FBI identification records under this authority must notify the individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in 28 CFR 16.34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so. A statement incorporating these use-and-challenge requirements will be placed on all records disseminated under this program. This policy is intended to ensure that all relevant criminal record information is made available to provide for the public safety and, further, to protect the interests of the prospective employee/licensee who may be affected by the information or lack of information in an identification record.

Official Citation:
[Order No. 2258-99, 64 FR 52229, Sept. 28, 1999]

Page 688
The guidelines set forth below are intended as a statement of policy of the Department of Justice and will be applied by the Department in exercising its responsibilities under Federal law relating to equal employment opportunity.

Uniform Guidelines on Employee Selection Procedures (1978)

Note:
These guidelines are issued jointly by four agencies. Separate official adoptions follow the guidelines in this part IV as follows: Civil Service Commission, Department of Justice, Equal Employment Opportunity Commission, Department of Labor.

For official citation see section 18 of these guidelines.

Table of Contents
general principles
1. Statement of Purpose
   A. Need for Uniformity—Issuing Agencies
   B. Purpose of Guidelines
   C. Relation to Prior Guidelines
2. Scope
   A. Application of Guidelines
   B. Employment Decisions
   C. Selection Procedures
   D. Limitations
   E. Indian Preference Not Affected
3. Discrimination Defined: Relationship Between Use of Selection Procedures and Discrimination
   A. Procedure Having Adverse Impact Constitutes Discrimination Unless Justified
B. Consideration of Suitable Alternative Selection Procedures

4. Information on Impact
A. Records Concerning Impact
B. Applicable Race, Sex and Ethnic Groups For Record Keeping
C. Evaluation of Selection Rates. The “Bottom Line”
D. Adverse Impact And The “Four-Fifths Rule”
E. Consideration of User's Equal Employment Opportunity Posture

5. General Standards for Validity Studies
A. Acceptable types of Validity Studies
B. Criterion-Related, Content, and Construct Validity
C. Guidelines Are Consistent with Professional Standards
D. Need For Documentation of Validity
E. Accuracy and Standardization
F. Caution Against Selection on Basis of Knowledges, Skills or Abilities Learned in Brief Orientation Period

G. Method of Use of Selection Procedures
H. Cutoff Scores
I. Use of Selection Procedures for Higher Level Jobs
J. Interim Use of Selection Procedures
K. Review of Validity Studies for Currency

6. Use of Selection Procedures Which Have Not Been Validated
A. Use of Alternate Selection Procedures to Eliminate Adverse Impact
B. Where Validity Studies Cannot or Need Not Be Performed

(1) Where Informal or Unscored Procedures Are Used
(2) Where Formal And Scored Procedures Are Used

7. Use of Other Validity Studies

A. Validity Studies not Conducted by the User
B. Use of Criterion-Related Validity Evidence from Other Sources

(1) Validity Evidence
(2) Job Similarity
(3) Fairness Evidence

C. Validity Evidence from Multi-Unit Study

D. Other Significant Variables

8. Cooperative Studies

A. Encouragement of Cooperative Studies
B. Standards for Use of Cooperative Studies

9. No Assumption of Validity

A. Unacceptable Substitutes for Evidence of Validity
B. Encouragement of Professional Supervision

10. Employment Agencies and Employment Services

A. Where Selection Procedures Are Devised by Agency
B. Where Selection Procedures Are Devised Elsewhere

11. Disparate Treatment

12. Retesting of Applicants

13. Affirmative Action
A. Affirmative Action Obligations

B. Encouragement of Voluntary Affirmative Action Programs

technical standards
14. Technical Standards for Validity Studies

A. Validity Studies Should be Based on Review of Information about the Job

B. Technical Standards for Criterion-Related Validity Studies

(1) Technical Feasibility

(2) Analysis of the Job

(3) Criterion Measures

(4) Representativeness of the Sample

(5) Statistical Relationships

(6) Operational Use of Selection Procedures

(7) Over-Statement of Validity Findings

(8) Fairness

(a) Unfairness Defined

(b) Investigation of Fairness

(c) General Considerations in Fairness Investigations

(d) When Unfairness Is Shown

(e) Technical Feasibility of Fairness Studies

(f) Continued Use of Selection Procedures When Fairness Studies not Feasible

C. Technical Standards for Content Validity Studies

(1) Appropriateness of Content Validity Studies

(2) Job Analysis for Content Validity
(3) Development of Selection Procedure
(4) Standards For Demonstrating Content Validity
(5) Reliability
(6) Prior Training or Experience
(7) Training Success
(8) Operational Use
(9) Ranking Based on Content Validity Studies

D. Technical Standards For Construct Validity Studies

(1) Appropriateness of Construct Validity Studies
(2) Job Analysis For Construct Validity Studies
(3) Relationship to the Job
(4) Use of Construct Validity Study Without New Criterion-Related Evidence
(a) Standards for Use
(b) Determination of Common Work Behaviors
documentation of impact and validity evidence

15. Documentation of Impact and Validity Evidence

A. Required Information
(1) Simplified Recordkeeping for Users With Less Than 100 Employees
(2) Information on Impact
(a) Collection of Information on Impact
(b) When Adverse Impact Has Been Eliminated in The Total Selection Process
(c) When Data Insufficient to Determine Impact
(3) Documentation of Validity Evidence

(a) Type of Evidence

(b) Form of Report

(c) Completeness

B. Criterion-Related Validity Studies

(1) User(s), Location(s), and Date(s) of Study

(2) Problem and Setting

(3) Job Analysis or Review of Job Information

(4) Job Titles and Codes

(5) Criterion Measures

(6) Sample Description

(7) Description of Selection Procedure

(8) Techniques and Results

(9) Alternative Procedures Investigated

(10) Uses and Applications

(11) Source Data

(12) Contact Person

(13) Accuracy and Completeness

C. Content Validity Studies

(1) User(s), Location(s), and Date(s) of Study

(2) Problem and Setting

(3) Job Analysis—Content of the Job

(4) Selection Procedure and its Content
(5) Relationship Between Selection Procedure and the Job

(6) Alternative Procedures Investigated

(7) Uses and Applications

(8) Contact Person

(9) Accuracy and Completeness

D. Construct Validity Studies

(1) User(s), Location(s), and Date(s) of Study

(2) Problem and Setting

(3) Construct Definition

(4) Job Analysis

(5) Job Titles and Codes

(6) Selection Procedure

(7) Relationship to Job Performance

(8) Alternative Procedures Investigated

(9) Uses and Applications

(10) Accuracy and Completeness

(11) Source Data

(12) Contact Person

E. Evidence of Validity from Other Studies

(1) Evidence from Criterion-Related Validity Studies

(a) Job Information

(b) Relevance of Criteria

(c) Other Variables
(d) Use of the Selection Procedure

(e) Bibliography

(2) Evidence from Content Validity Studies

(3) Evidence from Construct Validity Studies

F. Evidence of Validity from Cooperative Studies

G. Selection for Higher Level Jobs

H. Interim Use of Selection Procedures

definitions

16. Definitions

appendix

17. Policy Statement on Affirmative Action (see Section 13B)

18. Citations

General Principles

Section

1. Statement of purpose

—A. Need for uniformity—Issuing agencies.

The Federal government's need for a uniform set of principles on the question of the use of tests and other selection procedures has long been recognized. The Equal Employment Opportunity Commission, the Civil Service Commission, the Department of Labor, and the Department of Justice jointly have adopted these uniform guidelines to meet that need, and to apply the same principles to the Federal Government as are applied to other employers.

B. Purpose of guidelines.

These guidelines incorporate a single set of principles which are designed to assist employers, labor organizations, employment agencies, and licensing and certification boards to comply with requirements of Federal law prohibiting employment practices which discriminate on grounds of race, color, religion, sex, and national origin. They are designed to provide a framework for determining the proper use of tests and other selection procedures. These guidelines do not require a user to conduct validity studies of selection procedures where no adverse impact results. However, all users are encouraged to use selection procedures which are valid, especially users operating under merit principles.
C. Relation to prior guidelines.
These guidelines are based upon and supersede previously issued guidelines on employee selection procedures. These guidelines have been built upon court decisions, the previously issued guidelines of the agencies, and the practical experience of the agencies, as well as the standards of the psychological profession. These guidelines are intended to be consistent with existing law.

Sec. 2. Scope
—A. Application of guidelines.
These guidelines will be applied by the Equal Employment Opportunity Commission in the enforcement of title VII of the Civil Rights Act of 1964, as amended by the Equal Employment Opportunity Act of 1972 (hereinafter “Title VII”); by the Department of Labor, and the contract compliance agencies until the transfer of authority contemplated by the President’s Reorganization Plan No. 1 of 1978, in the administration and enforcement of Executive Order 11246, as amended by Executive Order 11375 (hereinafter “Executive Order 11246”); by the Civil Service Commission and other Federal agencies subject to section 717 of title VII; by the Civil Service Commission in exercising its responsibilities toward State and local governments under section 208(b)(1) of the Intergovernmental-Personnel Act; by the Department of Justice in exercising its responsibilities under Federal law; by the Office of Revenue Sharing of the Department of the Treasury under the State and Local Fiscal Assistance Act of 1972, as amended; and by any other Federal agency which adopts them.

B. Employment decisions.
These guidelines apply to tests and other selection procedures which are used as a basis for any employment decision. Employment decisions include but are not limited to hiring, promotion, demotion, membership (for example, in a labor organization), referral, retention, and licensing and certification, to the extent that licensing and certification may be covered by Federal equal employment opportunity law. Other selection decisions, such as selection for training or transfer, may also be considered employment decisions if they lead to any of the decisions listed above.

C. Selection procedures.
These guidelines apply only to selection procedures which are used as a basis for making employment decisions. For example, the use of recruiting procedures designed to attract members of a particular race, sex, or ethnic group, which were previously denied employment opportunities or which are currently underutilized, may be necessary to bring an employer into compliance with Federal law, and is frequently an essential element of any effective affirmative action program; but recruitment practices are not considered by these guidelines to be selection procedures. Similarly, these guidelines do not pertain to the question of the lawfulness of a seniority system within the meaning of section
703(h), Executive Order 11246 or other provisions of Federal law or regulation, except to the extent that such systems utilize selection procedures to determine qualifications or abilities to perform the job. Nothing in these guidelines is intended or should be interpreted as discouraging the use of a selection procedure for the purpose of determining qualifications or for the purpose of selection on the basis of relative qualifications, if the selection procedure had been validated in accord with these guidelines for each such purpose for which it is to be used.

D. Limitations.
These guidelines apply only to persons subject to title VII, Executive Order 11246, or other equal employment opportunity requirements of Federal law. These guidelines do not apply to responsibilities under the Age Discrimination in Employment Act of 1967, as amended, not to discriminate on the basis of age, or under sections 501, 503, and 504 of the Rehabilitation Act of 1973, not to discriminate on the basis of handicap.

E. Indian preference not affected.
These guidelines do not restrict any obligation imposed or right granted by Federal law to users to extend a preference in employment to Indians living on or near an Indian reservation in connection with employment opportunities on or near an Indian reservation.

Sec. 3. Discrimination defined: Relationship between use of selection procedures and discrimination
—A. Procedure having adverse impact constitutes discrimination unless justified. The use of any selection procedure which has an adverse impact on the hiring, promotion, or other employment or membership opportunities of members of any race, sex, or ethnic group will be considered to be discriminatory and inconsistent with these guidelines, unless the procedure has been validated in accordance with these guidelines, or the provisions of section 6 below are satisfied.

B. Consideration of suitable alternative selection procedures.
Where two or more selection procedures are available which serve the user's legitimate interest in efficient and trustworthy workmanship, and which are substantially equally valid for a given purpose, the user should use the procedure which has been demonstrated to have the lesser adverse impact. Accordingly, whenever a validity study is called for by these guidelines, the user should include, as a part of the validity study, an investigation of suitable alternative selection procedures and suitable alternative methods of using the selection procedure which have as little adverse impact as possible, to determine the appropriateness of using or validating them in accord with these guidelines. If a user has made a reasonable effort to become aware of such alternative procedures
and validity has been demonstrated in accord with these guidelines, the use of the test or other selection procedure may continue until such time as it should reasonably be reviewed for currency. Whenever the user is shown an alternative selection procedure with evidence of less adverse impact and substantial evidence of validity for the same job in similar circumstances, the user should investigate it to determine the appropriateness of using or validating it in accord with these guidelines. This subsection is not intended to preclude the combination of procedures into a significantly more valid procedure, if the use of such a combination has been shown to be in compliance with the guidelines.

Sec.
4. Information on impact
   —A. Records concerning impact.
   Each user should maintain and have available for inspection records or other information which will disclose the impact which its tests and other selection procedures have upon employment opportunities of persons by identifiable race, sex, or ethnic group as set forth in paragraph B below in order to determine compliance with these guidelines. Where there are large numbers of applicants and procedures are administered frequently, such information may be retained on a sample basis, provided that the sample is appropriate in terms of the applicant population and adequate in size.

B. Applicable race, sex, and ethnic groups for recordkeeping.
The records called for by this section are to be maintained by sex, and the following races and ethnic groups: Blacks (Negroes), American Indians (including Alaskan Natives), Asians (including Pacific Islanders), Hispanic (including persons of Mexican, Puerto Rican, Cuban, Central or South American, or other Spanish origin or culture regardless of race), whites (Caucasians) other than Hispanic, and totals. The race, sex, and ethnic classifications called for by this section are consistent with the Equal Employment Opportunity Standard Form 100, Employer Information Report EEO-1 series of reports. The user should adopt safeguards to insure that the records required by this paragraph are used for appropriate purposes such as determining adverse impact, or (where required) for developing and monitoring affirmative action programs, and that such records are not used improperly. See sections 4E and 17(4), below.

C. Evaluation of selection rates. The “bottom line.”
If the information called for by sections 4A and B above shows that the total selection process for a job has an adverse impact, the individual components of the selection process should be evaluated for adverse impact. If this information shows that the total selection process does not have an adverse impact, the Federal enforcement agencies, in the exercise of their administrative and prosecutorial discretion, in usual circumstances, will not expect a user to evaluate the individual components for adverse impact, or to validate such individual components, and will not take enforcement action based upon adverse impact of any component of that process, including the separate parts of a multipart
selection procedure or any separate procedure that is used as an alternative method of selection. However, in the following circumstances the Federal enforcement agencies will expect a user to evaluate the individual components for adverse impact and may, where appropriate, take enforcement action with respect to the individual components: (1) Where the selection procedure is a significant factor in the continuation of patterns of assignments of incumbent employees caused by prior discriminatory employment practices, (2) where the weight of court decisions or administrative interpretations hold that a specific procedure (such as height or weight requirements or no-arrest records) is not job related in the same or similar circumstances. In unusual circumstances, other than those listed in (1) and (2) above, the Federal enforcement agencies may request a user to evaluate the individual components for adverse impact and may, where appropriate, take enforcement action with respect to the individual component.

D. Adverse impact and the “four-fifths rule.”
A selection rate for any race, sex, or ethnic group which is less than four-fifths (4/5) (or eighty percent) of the rate for the group with the highest rate will generally be regarded by the Federal enforcement agencies as evidence of adverse impact, while a greater than four-fifths rate will generally not be regarded by Federal enforcement agencies as evidence of adverse impact. Smaller differences in selection rate may nevertheless constitute adverse impact, where they are significant in both statistical and practical terms or where a user's actions have discouraged applicants disproportionately on grounds of race, sex, or ethnic group. Greater differences in selection rate may not constitute adverse impact where the differences are based on small numbers and are not statistically significant, or where special recruiting or other programs cause the pool of minority or female candidates to be atypical of the normal pool of applicants from that group. Where the user's evidence concerning the impact of a selection procedure indicates adverse impact but is based upon numbers which are too small to be reliable, evidence concerning the impact of the procedure over a longer period of time and/or evidence concerning the impact which the selection procedure had when used in the same manner in similar circumstances elsewhere may be considered in determining adverse impact. Where the user has not maintained data on adverse impact as required by the documentation section of applicable guidelines, the Federal enforcement agencies may draw an inference of adverse impact of the selection process from the failure of the user to maintain such data, if the user has an underutilization of a group in the job category, as compared to the group's representation in the relevant labor market or, in the case of jobs filled from within, the applicable work force.

E. Consideration of user's equal employment opportunity posture.
In carrying out their obligations, the Federal enforcement agencies will consider the general posture of the user with respect to equal employment opportunity for the job or group of jobs in question. Where a user has adopted an affirmative action program, the Federal enforcement agencies will consider the provisions of
that program, including the goals and timetables which the user has adopted and the progress which the user has made in carrying out that program and in meeting the goals and timetables. While such affirmative action programs may in design and execution be race, color, sex, or ethnic conscious, selection procedures under such programs should be based upon the ability or relative ability to do the work.

Sec. 5. General standards for validity studies
   —A. Acceptable types of validity studies.
   For the purposes of satisfying these guidelines, users may rely upon criterion-related validity studies, content validity studies or construct validity studies, in accordance with the standards set forth in the technical standards of these guidelines, section 14 below. New strategies for showing the validity of selection procedures will be evaluated as they become accepted by the psychological profession.

   B. Criterion-related, content, and construct validity.
   Evidence of the validity of a test or other selection procedure by a criterion-related validity study should consist of empirical data demonstrating that the selection procedure is predictive of or significantly correlated with important elements of job performance. See section 14B below. Evidence of the validity of a test or other selection procedure by a content validity study should consist of data showing that the content of the selection procedure is representative of important aspects of performance on the job for which the candidates are to be evaluated. See section 14C below. Evidence of the validity of a test or other selection procedure through a construct validity study should consist of data showing that the procedure measures the degree to which candidates have identifiable characteristics which have been determined to be important in successful performance in the job for which the candidates are to be evaluated. See section 14D below.

   C. Guidelines are consistent with professional standards.
   The provisions of these guidelines relating to validation of selection procedures are intended to be consistent with generally accepted professional standards for evaluating standardized tests and other selection procedures, such as those described in the Standards for Educational and Psychological Tests prepared by a joint committee of the American Psychological Association, the American Educational Research Association, and the National Council on Measurement in Education (American Psychological Association, Washington, DC, 1974) (hereinafter “A.P.A. Standards”) and standard textbooks and journals in the field of personnel selection.

   D. Need for documentation of validity.
   For any selection procedure which is part of a selection process which has an adverse impact and which selection procedure has an adverse impact, each user
should maintain and have available such documentation as is described in section 15 below.

E. Accuracy and standardization.
Validity studies should be carried out under conditions which assure insofar as possible the adequacy and accuracy of the research and the report. Selection procedures should be administered and scored under standardized conditions.

F. Caution against selection on basis of knowledges, skills, or ability learned in brief orientation period.
In general, users should avoid making employment decisions on the basis of measures of knowledges, skills, or abilities which are normally learned in a brief orientation period, and which have an adverse impact.

G. Method of use of selection procedures.
The evidence of both the validity and utility of a selection procedure should support the method the user chooses for operational use of the procedure, if that method of use has a greater adverse impact than another method of use. Evidence which may be sufficient to support the use of a selection procedure on a pass/fail (screening) basis may be insufficient to support the use of the same procedure on a ranking basis under these guidelines. Thus, if a user decides to use a selection procedure on a ranking basis, and that method of use has a greater adverse impact than use on an appropriate pass/fail basis (see section 5H below), the user should have sufficient evidence of validity and utility to support the use on a ranking basis. See sections 3B, 14B (5) and (6), and 14C (8) and (9).

H. Cutoff scores.
Where cutoff scores are used, they should normally be set so as to be reasonable and consistent with normal expectations of acceptable proficiency within the work force. Where applicants are ranked on the basis of properly validated selection procedures and those applicants scoring below a higher cutoff score than appropriate in light of such expectations have little or no chance of being selected for employment, the higher cutoff score may be appropriate, but the degree of adverse impact should be considered.

I. Use of selection procedures for higher level jobs.
If job progression structures are so established that employees will probably, within a reasonable period of time and in a majority of cases, progress to a higher level, it may be considered that the applicants are being evaluated for a job or jobs at the higher level. However, where job progression is not so nearly automatic, or the time span is such that higher level jobs or employees' potential may be expected to change in significant ways, it should be considered that applicants are being evaluated for a job at or near the entry level. A “reasonable period of time” will vary for different jobs and employment situations but will seldom be more than 5 years. Use of selection procedures to evaluate applicants for a higher level job would not be appropriate:
(1) If the majority of those remaining employed do not progress to the
higher level job;

(2) If there is a reason to doubt that the higher level job will continue to
require essentially similar skills during the progression period; or

(3) If the selection procedures measure knowledges, skills, or abilities
required for advancement which would be expected to develop principally from
the training or experience on the job.

J. Interim use of selection procedures.
Users may continue the use of a selection procedure which is not at the moment
fully supported by the required evidence of validity, provided:(1) The user has
available substantial evidence of validity, and (2) the user has in progress, when
technically feasible, a study which is designed to produce the additional evidence
required by these guidelines within a reasonable time. If such a study is not
technically feasible, see section 6B. If the study does not demonstrate validity,
this provision of these guidelines for interim use shall not constitute a defense in
any action, nor shall it relieve the user of any obligations arising under Federal
law.

K. Review of validity studies for currency.
Whenever validity has been shown in accord with these guidelines for the use of a
particular selection procedure for a job or group of jobs, additional studies need
not be performed until such time as the validity study is subject to review as
provided in section 3B above. There are no absolutes in the area of determining
the currency of a validity study. All circumstances concerning the study,
including the validation strategy used, and changes in the relevant labor market
and the job should be considered in the determination of when a validity study is
outdated.

Sec.
6. Use of selection procedures which have not been validated
—A. Use of alternate selection procedures to eliminate adverse impact.
A user may choose to utilize alternative selection procedures in order to eliminate
adverse impact or as part of an affirmative action program. See section 13 below.
Such alternative procedures should eliminate the adverse impact in the total
selection process, should be lawful and should be as job related as possible.

B. Where validity studies cannot or need not be performed.
There are circumstances in which a user cannot or need not utilize the validation
techniques contemplated by these guidelines. In such circumstances, the user
should utilize selection procedures which are as job related as possible and which
will minimize or eliminate adverse impact, as set forth below.
(1) Where informal or unscored procedures are used.
When an informal or unscored selection procedure which has an adverse impact is utilized, the user should eliminate the adverse impact, or modify the procedure to one which is a formal, scored or quantified measure or combination of measures and then validate the procedure in accord with these guidelines, or otherwise justify continued use of the procedure in accord with Federal law.

(2) Where formal and scored procedures are used.
When a formal and scored selection procedure is used which has an adverse impact, the validation techniques contemplated by these guidelines usually should be followed if technically feasible. Where the user cannot or need not follow the validation techniques anticipated by these guidelines, the user should either modify the procedure to eliminate adverse impact or otherwise justify continued use of the procedure in accord with Federal law.

Sec. 7. Use of other validity studies
—A. Validity studies not conducted by the user.
Users may, under certain circumstances, support the use of selection procedures by validity studies conducted by other users or conducted by test publishers or distributors and described in test manuals. While publishers of selection procedures have a professional obligation to provide evidence of validity which meets generally accepted professional standards (see section 5C above), users are cautioned that they are responsible for compliance with these guidelines. Accordingly, users seeking to obtain selection procedures from publishers and distributors should be careful to determine that, in the event the user becomes subject to the validity requirements of these guidelines, the necessary information to support validity has been determined and will be made available to the user.

B. Use of criterion-related validity evidence from other sources.
Criterion-related validity studies conducted by one test user, or described in test manuals and the professional literature, will be considered acceptable for use by another user when the following requirements are met:

(1) Validity evidence.
Evidence from the available studies meeting the standards of section 14B below clearly demonstrates that the selection procedure is valid;

(2) Job similarity.
The incumbents in the user's job and the incumbents in the job or group of jobs on which the validity study was conducted perform substantially the same major work behaviors, as shown by appropriate job analyses both on the job or group of
jobs on which the validity study was performed and on the job for which the selection procedure is to be used; and

(3) Fairness evidence.
The studies include a study of test fairness for each race, sex, and ethnic group which constitutes a significant factor in the borrowing user's relevant labor market for the job or jobs in question. If the studies under consideration satisfy (1) and (2) above but do not contain an investigation of test fairness, and it is not technically feasible for the borrowing user to conduct an internal study of test fairness, the borrowing user may utilize the study until studies conducted elsewhere meeting the requirements of these guidelines show test unfairness, or until such time as it becomes technically feasible to conduct an internal study of test fairness and the results of that study can be acted upon. Users obtaining selection procedures from publishers should consider, as one factor in the decision to purchase a particular selection procedure, the availability of evidence concerning test fairness.

C. Validity evidence from multiunit study.
if validity evidence from a study covering more than one unit within an organization satisfies the requirements of section 14B below, evidence of validity specific to each unit will not be required unless there are variables which are likely to affect validity significantly.

D. Other significant variables.
If there are variables in the other studies which are likely to affect validity significantly, the user may not rely upon such studies, but will be expected either to conduct an internal validity study or to comply with section 6 above.

Sec.
8. Cooperative studies
—A. Encouragement of cooperative studies.
The agencies issuing these guidelines encourage employers, labor organizations, and employment agencies to cooperate in research, development, search for lawful alternatives, and validity studies in order to achieve procedures which are consistent with these guidelines.

B. Standards for use of cooperative studies.
If validity evidence from a cooperative study satisfies the requirements of section 14 below, evidence of validity specific to each user will not be required unless there are variables in the user's situation which are likely to affect validity significantly.

Sec.
9. No assumption of validity
A. Unacceptable substitutes for evidence of validity.
Under no circumstances will the general reputation of a test or other selection procedures, its author or its publisher, or casual reports of its validity be accepted in lieu of evidence of validity. Specifically ruled out are: Assumptions of validity based on a procedure's name or descriptive labels; all forms of promotional literature; data bearing on the frequency of a procedure's usage; testimonial statements and credentials of sellers, users, or consultants; and other nonempirical or anecdotal accounts of selection practices or selection outcomes.

B. Encouragement of professional supervision.
Professional supervision of selection activities is encouraged but is not a substitute for documented evidence of validity. The enforcement agencies will take into account the fact that a thorough job analysis was conducted and that careful development and use of a selection procedure in accordance with professional standards enhance the probability that the selection procedure is valid for the job.

Sec.
10. Employment agencies and employment services
—A. Where selection procedures are devised by agency.
An employment agency, including private employment agencies and State employment agencies, which agrees to a request by an employer or labor organization to devise and utilize a selection procedure should follow the standards in these guidelines for determining adverse impact. If adverse impact exists the agency should comply with these guidelines. An employment agency is not relieved of its obligation herein because the user did not request such validation or has requested the use of some lesser standard of validation than is provided in these guidelines. The use of an employment agency does not relieve an employer or labor organization or other user of its responsibilities under Federal law to provide equal employment opportunity or its obligations as a user under these guidelines.

B. Where selection procedures are devised elsewhere.
Where an employment agency or service is requested to administer a selection procedure which has been devised elsewhere and to make referrals pursuant to the results, the employment agency or service should maintain and have available evidence of the impact of the selection and referral procedures which it administers. If adverse impact results the agency or service should comply with these guidelines. If the agency or service seeks to comply with these guidelines by reliance upon validity studies or other data in the possession of the employer, it should obtain and have available such information.

Sec.
The principles of disparate or unequal treatment must be distinguished from the concepts of validation. A selection procedure—even though validated against job performance in accordance with these guidelines—cannot be imposed upon members of a race, sex, or ethnic group where other employees, applicants, or members have not been subjected to that standard. Disparate treatment occurs where members of a race, sex, or ethnic group have been denied the same employment, promotion, membership, or other employment opportunities as have been available to other employees or applicants. Those employees or applicants who have been denied equal treatment, because of prior discriminatory practices or policies, must at least be afforded the same opportunities as had existed for other employees or applicants during the period of discrimination. Thus, the persons who were in the class of persons discriminated against during the period the user followed the discriminatory practices should be allowed the opportunity to qualify under less stringent selection procedures previously followed, unless the user demonstrates that the increased standards are required by business necessity. This section does not prohibit a user who has not previously followed merit standards from adopting merit standards which are in compliance with these guidelines; nor does it preclude a user who has previously used invalid or unvalidated selection procedures from developing and using procedures which are in accord with these guidelines.

Sec. 12. Retesting of applicants.
Users should provide a reasonable opportunity for retesting and reconsideration. Where examinations are administered periodically with public notice, such reasonable opportunity exists, unless persons who have previously been tested are precluded from retesting. The user may however take reasonable steps to preserve the security of its procedures.

Sec. 13. Affirmative action
—A. Affirmative action obligations.
The use of selection procedures which have been validated pursuant to these guidelines does not relieve users of any obligations they may have to undertake affirmative action to assure equal employment opportunity. Nothing in these guidelines is intended to preclude the use of lawful selection procedures which assist in remedying the effects of prior discriminatory practices, or the achievement of affirmative action objectives.

B. Encouragement of voluntary affirmative action programs.
These guidelines are also intended to encourage the adoption and implementation of voluntary affirmative action programs by users who have no obligation under Federal law to adopt them; but are not intended to impose any
new obligations in that regard. The agencies issuing and endorsing these
guidelines endorse for all private employers and reaffirm for all governmental
employers the Equal Employment Opportunity Coordinating Council’s “Policy
Statement on Affirmative Action Programs for State and Local Government
Agencies” (41 FR 38814, September 13, 1976). That policy statement is attached
hereto as appendix, section 17.

Technical Standards

Sec.
The following minimum standards, as applicable, should be met in conducting a
validity study. Nothing in these guidelines is intended to preclude the
development and use of other professionally acceptable techniques with respect
to validation of selection procedures. Where it is not technically feasible for a
user to conduct a validity study, the user has the obligation otherwise to comply
with these guidelines. See sections 6 and 7 above.

A. Validity studies should be based on review of information about the job.
Any validity study should be based upon a review of information about the job for
which the selection procedure is to be used. The review should include a job
analysis except as provided in section 14B(3) below with respect to criterion-
related validity. Any method of job analysis may be used if it provides the
information required for the specific validation strategy used.

B. Technical standards for criterion-related validity studies
(1) Technical feasibility.
Users choosing to validate a selection procedure by a criterion-related validity
strategy should determine whether it is technically feasible (as defined in section
16) to conduct such a study in the particular employment context. The
determination of the number of persons necessary to permit the conduct of a
meaningful criterion-related study should be made by the user on the basis of all
relevant information concerning the selection procedure, the potential sample
and the employment situation. Where appropriate, jobs with substantially the
same major work behaviors may be grouped together for validity studies, in order
to obtain an adequate sample. These guidelines do not require a user to hire or
promote persons for the purpose of making it possible to conduct a criterion-
related study.

(2) Analysis of the job.
There should be a review of job information to determine measures of work
behavior(s) or performance that are relevant to the job or group of jobs in
question. These measures or criteria are relevant to the extent that they represent
critical or important job duties, work behaviors or work outcomes as developed
from the review of job information. The possibility of bias should be considered
both in selection of the criterion measures and their application. In view of the
possibility of bias in subjective evaluations, supervisory rating techniques and instructions to raters should be carefully developed. All criterion measures and the methods for gathering data need to be examined for freedom from factors which would unfairly alter scores of members of any group. The relevance of criteria and their freedom from bias are of particular concern when there are significant differences in measures of job performance for different groups.

(3) Criterion measures.
Proper safeguards should be taken to insure that scores on selection procedures do not enter into any judgments of employee adequacy that are to be used as criterion measures. Whatever criteria are used should represent important or critical work behavior(s) or work outcomes. Certain criteria may be used without a full job analysis if the user can show the importance of the criteria to the particular employment context. These criteria include but are not limited to production rate, error rate, tardiness, absenteeism, and length of service. A standardized rating of overall work performance may be used where a study of the job shows that it is an appropriate criterion. Where performance in training is used as a criterion, success in training should be properly measured and the relevance of the training should be shown either through a comparison of the content of the training program with the critical or important work behavior(s) of the job(s), or through a demonstration of the relationship between measures of performance in training and measures of job performance. Measures of relative success in training include but are not limited to instructor evaluations, performance samples, or tests. Criterion measures consisting of paper and pencil tests will be closely reviewed for job relevance.

(4) Representativeness of the sample.
Whether the study is predictive or concurrent, the sample subjects should insofar as feasible be representative of the candidates normally available in the relevant labor market for the job or group of jobs in question, and should insofar as feasible include the races, sexes, and ethnic groups normally available in the relevant job market. In determining the representativeness of the sample in a concurrent validity study, the user should take into account the extent to which the specific knowledges or skills which are the primary focus of the test are those which employees learn on the job.

Where samples are combined or compared, attention should be given to see that such samples are comparable in terms of the actual job they perform, the length of time on the job where time on the job is likely to affect performance, and other relevant factors likely to affect validity differences; or that these factors are included in the design of the study and their effects identified.

(5) Statistical relationships.
The degree of relationship between selection procedure scores and criterion measures should be examined and computed, using professionally acceptable statistical procedures. Generally, a selection procedure is considered related to
the criterion, for the purposes of these guidelines, when the relationship between performance on the procedure and performance on the criterion measure is statistically significant at the 0.05 level of significance, which means that it is sufficiently high as to have a probability of no more than one (1) in twenty (20) to have occurred by chance. Absence of a statistically significant relationship between a selection procedure and job performance should not necessarily discourage other investigations of the validity of that selection procedure.

(6) Operational use of selection procedures.
Users should evaluate each selection procedure to assure that it is appropriate for operational use, including establishment of cutoff scores or rank ordering. Generally, if other factors remain the same, the greater the magnitude of the relationship (e.g., correlation coefficient) between performance on a selection procedure and one or more criteria of performance on the job, and the greater the importance and number of aspects of job performance covered by the criteria, the more likely it is that the procedure will be appropriate for use. Reliance upon a selection procedure which is significantly related to a criterion measure, but which is based upon a study involving a large number of subjects and has a low correlation coefficient will be subject to close review if it has a large adverse impact. Sole reliance upon a single selection instrument which is related to only one of many job duties or aspects of job performance will also be subject to close review. The appropriateness of a selection procedure is best evaluated in each particular situation and there are no minimum correlation coefficients applicable to all employment situations. In determining whether a selection procedure is appropriate for operational use the following considerations should also be taken into account: The degree of adverse impact of the procedure, the availability of other selection procedures of greater or substantially equal validity.

(7) Overstatement of validity findings.
Users should avoid reliance upon techniques which tend to overestimate validity findings as a result of capitalization on chance unless an appropriate safeguard is taken. Reliance upon a few selection procedures or criteria of successful job performance when many selection procedures or criteria of performance have been studied, or the use of optimal statistical weights for selection procedures computed in one sample, are techniques which tend to inflate validity estimates as a result of chance. Use of a large sample is one safeguard: Cross-validation is another.

(8) Fairness.
This section generally calls for studies of unfairness where technically feasible. The concept of fairness or unfairness of selection procedures is a developing concept. In addition, fairness studies generally require substantial numbers of employees in the job or group of jobs being studied. For these reasons, the Federal enforcement agencies recognize that the obligation to conduct studies of fairness imposed by the guidelines generally will be upon users or groups of users with a large number of persons in a job class, or test developers; and that small
users utilizing their own selection procedures will generally not be obligated to conduct such studies because it will be technically infeasible for them to do so.

(a) Unfairness defined. When members of one race, sex, or ethnic group characteristically obtain lower scores on a selection procedure than members of another group, and the differences in scores are not reflected in differences in a measure of job performance, use of the selection procedure may unfairly deny opportunities to members of the group that obtains the lower scores.

(b) Investigation of fairness. Where a selection procedure results in an adverse impact on a race, sex, or ethnic group identified in accordance with the classifications set forth in section 4 above and that group is a significant factor in the relevant labor market, the user generally should investigate the possible existence of unfairness for that group if it is technically feasible to do so. The greater the severity of the adverse impact on a group, the greater the need to investigate the possible existence of unfairness. Where the weight of evidence from other studies shows that the selection procedure predicts fairly for the group in question and for the same or similar jobs, such evidence may be relied on in connection with the selection procedure at issue.

(c) General considerations in fairness investigations. Users conducting a study of fairness should review the A.P.A. Standards regarding investigation of possible bias in testing. An investigation of fairness of a selection procedure depends on both evidence of validity and the manner in which the selection procedure is to be used in a particular employment context. Fairness of a selection procedure cannot necessarily be specified in advance without investigating these factors. Investigation of fairness of a selection procedure in samples where the range of scores on selection procedures or criterion measures is severely restricted for any subgroup sample (as compared to other subgroup samples) may produce misleading evidence of unfairness. That factor should accordingly be taken into account in conducting such studies and before reliance is placed on the results.

(d) When unfairness is shown. If unfairness is demonstrated through a showing that members of a particular group perform better or poorer on the job than their scores on the selection procedure would indicate through comparison with how members of other groups perform, the user may either revise or replace the selection instrument in accordance with these guidelines, or may continue to use the selection instrument operationally with appropriate revisions in its use to assure compatibility between the probability of successful job performance and the probability of being selected.

(e) Technical feasibility of fairness studies.
In addition to the general conditions needed for technical feasibility for the conduct of a criterion-related study (see section 16, below) an investigation of fairness requires the following:

(i) An adequate sample of persons in each group available for the study to achieve findings of statistical significance. Guidelines do not require a user to hire or promote persons on the basis of group classifications for the purpose of making it possible to conduct a study of fairness; but the user has the obligation otherwise to comply with these guidelines.

(ii) The samples for each group should be comparable in terms of the actual job they perform, length of time on the job where time on the job is likely to affect performance, and other relevant factors likely to affect validity differences; or such factors should be included in the design of the study and their effects identified.

(f) Continued use of selection procedures when fairness studies not feasible.
If a study of fairness should otherwise be performed, but is not technically feasible, a selection procedure may be used which has otherwise met the validity standards of these guidelines, unless the technical infeasibility resulted from discriminatory employment practices which are demonstrated by facts other than past failure to conform with requirements for validation of selection procedures. However, when it becomes technically feasible for the user to perform a study of fairness and such a study is otherwise called for, the user should conduct the study of fairness.

C. Technical standards for content validity studies
(1) Appropriateness of content validity studies.
Users choosing to validate a selection procedure by a content validity strategy should determine whether it is appropriate to conduct such a study in the particular employment context. A selection procedure can be supported by a content validity strategy to the extent that it is a representative sample of the content of the job. Selection procedures which purport to measure knowledges, skills, or abilities may in certain circumstances be justified by content validity, although they may not be representative samples, if the knowledge, skill, or ability measured by the selection procedure can be operationally defined as provided in section 14C(4) below, and if that knowledge, skill, or ability is a necessary prerequisite to successful job performance.

A selection procedure based upon inferences about mental processes cannot be supported solely or primarily on the basis of content validity. Thus, a content strategy is not appropriate for demonstrating the validity of selection procedures which purport to measure traits or constructs, such as intelligence, aptitude, personality, commonsense, judgment, leadership, and spatial ability. Content validity is also not an appropriate strategy when the selection procedure involves
knowledges, skills, or abilities which an employee will be expected to learn on the job.

(2) Job analysis for content validity. There should be a job analysis which includes an analysis of the important work behavior(s) required for successful performance and their relative importance and, if the behavior results in work product(s), an analysis of the work product(s). Any job analysis should focus on the work behavior(s) and the tasks associated with them. If work behavior(s) are not observable, the job analysis should identify and analyze those aspects of the behavior(s) that can be observed and the observed work products. The work behavior(s) selected for measurement should be critical work behavior(s) and/or important work behavior(s) constituting most of the job.

(3) Development of selection procedures. A selection procedure designed to measure the work behavior may be developed specifically from the job and job analysis in question, or may have been previously developed by the user, or by other users or by a test publisher.

(4) Standards for demonstrating content validity. To demonstrate the content validity of a selection procedure, a user should show that the behavior(s) demonstrated in the selection procedure are a representative sample of the behavior(s) of the job in question or that the selection procedure provides a representative sample of the work product of the job. In the case of a selection procedure measuring a knowledge, skill, or ability, the knowledge, skill, or ability being measured should be operationally defined. In the case of a selection procedure measuring a knowledge, the knowledge being measured should be operationally defined as that body of learned information which is used in and is a necessary prerequisite for observable aspects of work behavior of the job. In the case of skills or abilities, the skill or ability being measured should be operationally defined in terms of observable aspects of work behavior of the job. For any selection procedure measuring a knowledge, skill, or ability the user should show that (a) the selection procedure measures and is a representative sample of that knowledge, skill, or ability; and (b) that knowledge, skill, or ability is used in and is a necessary prerequisite to performance of critical or important work behavior(s). In addition, to be content valid, a selection procedure measuring a skill or ability should either closely approximate an observable work behavior, or its product should closely approximate an observable work product. If a test purports to sample a work behavior or to provide a sample of a work product, the manner and setting of the selection procedure and its level and complexity should closely approximate the work situation. The closer the content and the context of the selection procedure are to work samples or work behaviors, the stronger is the basis for showing content validity. As the content of the selection procedure less resembles a work behavior, or the setting and manner of the administration of the selection procedure less resemble the work situation, or
the result less resembles a work product, the less likely the selection procedure is to be content valid, and the greater the need for other evidence of validity.

(5) Reliability. The reliability of selection procedures justified on the basis of content validity should be a matter of concern to the user. Whenever it is feasible, appropriate statistical estimates should be made of the reliability of the selection procedure.

(6) Prior training or experience. A requirement for or evaluation of specific prior training or experience based on content validity, including a specification of level or amount of training or experience, should be justified on the basis of the relationship between the content of the training or experience and the content of the job for which the training or experience is to be required or evaluated. The critical consideration is the resemblance between the specific behaviors, products, knowledges, skills, or abilities in the experience or training and the specific behaviors, products, knowledges, skills, or abilities required on the job, whether or not there is close resemblance between the experience or training as a whole and the job as a whole.

(7) Content validity of training success. Where a measure of success in a training program is used as a selection procedure and the content of a training program is justified on the basis of content validity, the use should be justified on the relationship between the content of the training program and the content of the job.

(8) Operational use. A selection procedure which is supported on the basis of content validity may be used for a job if it represents a critical work behavior (i.e., a behavior which is necessary for performance of the job) or work behaviors which constitute most of the important parts of the job.

(9) Ranking based on content validity studies. If a user can show, by a job analysis or otherwise, that a higher score on a content valid selection procedure is likely to result in better job performance, the results may be used to rank persons who score above minimum levels. Where a selection procedure supported solely or primarily by content validity is used to rank job candidates, the selection procedure should measure those aspects of performance which differentiate among levels of job performance.

D. Technical standards for construct validity studies

(1) Appropriateness of construct validity studies. Construct validity is a more complex strategy than either criterion-related or content validity. Construct validation is a relatively new and developing procedure in the employment field, and there is at present a lack of substantial literature extending the concept to employment practices. The user should be
aware that the effort to obtain sufficient empirical support for construct validity is both an extensive and arduous effort involving a series of research studies, which include criterion related validity studies and which may include content validity studies. Users choosing to justify use of a selection procedure by this strategy should therefore take particular care to assure that the validity study meets the standards set forth below.

(2) Job analysis for construct validity studies.
There should be a job analysis. This job analysis should show the work behavior(s) required for successful performance of the job, or the groups of jobs being studied, the critical or important work behavior(s) in the job or group of jobs being studied, and an identification of the construct(s) believed to underlie successful performance of these critical or important work behaviors in the job or jobs in question. Each construct should be named and defined, so as to distinguish it from other constructs. If a group of jobs is being studied the jobs should have in common one or more critical or important work behaviors at a comparable level of complexity.

(3) Relationship to the job.
A selection procedure should then be identified or developed which measures the construct identified in accord with paragraph (2) above. The user should show by empirical evidence that the selection procedure is validly related to the construct and that the construct is validly related to the performance of critical or important work behavior(s). The relationship between the construct as measured by the selection procedure and the related work behavior(s) should be supported by empirical evidence from one or more criterion-related studies involving the job or jobs in question which satisfy the provisions of section 14B above.

(4) Use of construct validity study without new criterion-related evidence
—(a) Standards for use.
Until such time as professional literature provides more guidance on the use of construct validity in employment situations, the Federal agencies will accept a claim of construct validity without a criterion-related study which satisfies section 14B above only when the selection procedure has been used elsewhere in a situation in which a criterion-related study has been conducted and the use of a criterion-related validity study in this context meets the standards for transportability of criterion-related validity studies as set forth above in section 7. However, if a study pertains to a number of jobs having common critical or important work behaviors at a comparable level of complexity, and the evidence satisfies paragraphs 14B (2) and (3) above for those jobs with criterion-related validity evidence for those jobs, the selection procedure may be used for all the jobs to which the study pertains. If construct validity is to be generalized to other jobs or groups of jobs not in the group studied, the Federal enforcement agencies will expect at a minimum additional empirical research evidence meeting the standards of paragraphs section 14B (2) and (3) above for the additional jobs or groups of jobs.
(b) Determination of common work behaviors.
In determining whether two or more jobs have one or more work behavior(s) in
common, the user should compare the observed work behavior(s) in each of the
jobs and should compare the observed work product(s) in each of the jobs. If
neither the observed work behavior(s) in each of the jobs nor the observed work
product(s) in each of the jobs are the same, the Federal enforcement agencies will
presume that the work behavior(s) in each job are different. If the work behaviors
are not observable, then evidence of similarity of work products and any other
relevant research evidence will be considered in determining whether the work
behavior(s) in the two jobs are the same.

Documentation of Impact and Validity Evidence

Sec.
15. Documentation of impact and validity evidence
   —A. Required information.
Users of selection procedures other than those users complying with section
15A(1) below should maintain and have available for each job information on
adverse impact of the selection process for that job and, where it is determined a
selection process has an adverse impact, evidence of validity as set forth below.

   (1) Simplified recordkeeping for users with less than 100 employees.
   In order to minimize recordkeeping burdens on employers who employ one
   hundred (100) or fewer employees, and other users not required to file EEO-1, et
   seq., reports, such users may satisfy the requirements of this section 15 if they
   maintain and have available records showing, for each year:
   
   (a) The number of persons hired, promoted, and terminated for each job, by sex,
   and where appropriate by race and national origin;

   (b) The number of applicants for hire and promotion by sex and where
   appropriate by race and national origin; and

   (c) The selection procedures utilized (either standardized or not standardized).

   These records should be maintained for each race or national origin group (see
section 4 above) constituting more than two percent (2%) of the labor force in the
relevant labor area. However, it is not necessary to maintain records by race
and/or national origin (see section 4 above) if one race or national origin group in
the relevant labor area constitutes more than ninety-eight percent (98%) of the
labor force in the area. If the user has reason to believe that a selection procedure
has an adverse impact, the user should maintain any available evidence of
validity for that procedure (see sections 7A and 8).

   (2) Information on impact
—(a) Collection of information on impact. Users of selection procedures other than those complying with section 15A(1) above should maintain and have available for each job records or other information showing whether the total selection process for that job has an adverse impact on any of the groups for which records are called for by sections 4B above. Adverse impact determinations should be made at least annually for each such group which constitutes at least 2 percent of the labor force in the relevant labor area or 2 percent of the applicable workforce. Where a total selection process for a job has an adverse impact, the user should maintain and have available records or other information showing which components have an adverse impact. Where the total selection process for a job does not have an adverse impact, information need not be maintained for individual components except in circumstances set forth in subsection 15A(2)(b) below. If the determination of adverse impact is made using a procedure other than the “four-fifths rule,” as defined in the first sentence of section 4D above, a justification, consistent with section 4D above, for the procedure used to determine adverse impact should be available.

(b) When adverse impact has been eliminated in the total selection process. Whenever the total selection process for a particular job has had an adverse impact, as defined in section 4 above, in any year, but no longer has an adverse impact, the user should maintain and have available the information on individual components of the selection process required in the preceding paragraph for the period in which there was adverse impact. In addition, the user should continue to collect such information for at least two (2) years after the adverse impact has been eliminated.

(c) When data insufficient to determine impact. Where there has been an insufficient number of selections to determine whether there is an adverse impact of the total selection process for a particular job, the user should continue to collect, maintain and have available the information on individual components of the selection process required in section 15(A)(2)(a) above until the information is sufficient to determine that the overall selection process does not have an adverse impact as defined in section 4 above, or until the job has changed substantially.

(3) Documentation of validity evidence
—(a) Types of evidence. Where a total selection process has an adverse impact (see section 4 above) the user should maintain and have available for each component of that process which has an adverse impact, one or more of the following types of documentation evidence:

(i) Documentation evidence showing criterion-related validity of the selection procedure (see section 15B, below).
(ii) Documentation evidence showing content validity of the selection procedure (see section 15C, below).

(iii) Documentation evidence showing construct validity of the selection procedure (see section 15D, below).

(iv) Documentation evidence from other studies showing validity of the selection procedure in the user's facility (see section 15E, below).

(v) Documentation evidence showing why a validity study cannot or need not be performed and why continued use of the procedure is consistent with Federal law.

(b) Form of report.
This evidence should be compiled in a reasonably complete and organized manner to permit direct evaluation of the validity of the selection procedure. Previously written employer or consultant reports of validity, or reports describing validity studies completed before the issuance of these guidelines are acceptable if they are complete in regard to the documentation requirements contained in this section, or if they satisfied requirements of guidelines which were in effect when the validity study was completed. If they are not complete, the required additional documentation should be appended. If necessary information is not available the report of the validity study may still be used as documentation, but its adequacy will be evaluated in terms of compliance with the requirements of these guidelines.

(c) Completeness.
In the event that evidence of validity is reviewed by an enforcement agency, the validation reports completed after the effective date of these guidelines are expected to contain the information set forth below. Evidence denoted by use of the word “(Essential)” is considered critical. If information denoted essential is not included, the report will be considered incomplete unless the user affirmatively demonstrates either its unavailability due to circumstances beyond the user's control or special circumstances of the user's study which make the information irrelevant. Evidence not so denoted is desirable but its absence will not be a basis for considering a report incomplete. The user should maintain and have available the information called for under the heading “Source Data” in sections 15B(11) and 15D(11). While it is a necessary part of the study, it need not be submitted with the report. All statistical results should be organized and presented in tabular or graphic form to the extent feasible.

B. Criterion-related validity studies.
Reports of criterion-related validity for a selection procedure should include the following information:

(1) User(s), location(s), and date(s) of study.
Dates and location(s) of the job analysis or review of job information, the date(s) and location(s) of the administration of the selection procedures and collection of criterion data, and the time between collection of data on selection procedures and criterion measures should be provided (Essential). If the study was conducted at several locations, the address of each location, including city and State, should be shown.

(2) Problem and setting.
An explicit definition of the purpose(s) of the study and the circumstances in which the study was conducted should be provided. A description of existing selection procedures and cutoff scores, if any, should be provided.

(3) Job analysis or review of job information.
A description of the procedure used to analyze the job or group of jobs, or to review the job information should be provided (Essential). Where a review of job information results in criteria which may be used without a full job analysis (see section 14B(3)), the basis for the selection of these criteria should be reported (Essential). Where a job analysis is required a complete description of the work behavior(s) or work outcome(s), and measures of their criticality or importance should be provided (Essential). The report should describe the basis on which the behavior(s) or outcome(s) were determined to be critical or important, such as the proportion of time spent on the respective behaviors, their level of difficulty, their frequency of performance, the consequences of error, or other appropriate factors (Essential). Where two or more jobs are grouped for a validity study, the information called for in this subsection should be provided for each of the jobs, and the justification for the grouping (see section 14B(1)) should be provided (Essential).

(4) Job titles and codes.
It is desirable to provide the user's job title(s) for the job(s) in question and the corresponding job title(s) and code(s) from U.S. Employment Service's Dictionary of Occupational Titles.

(5) Criterion measures.
The bases for the selection of the criterion measures should be provided, together with references to the evidence considered in making the selection of criterion measures (essential). A full description of all criteria on which data were collected and means by which they were observed, recorded, evaluated, and quantified, should be provided (essential). If rating techniques are used as criterion measures, the appraisal form(s) and instructions to the rater(s) should be included as part of the validation evidence, or should be explicitly described and available (essential). All steps taken to insure that criterion measures are free from factors which would unfairly alter the scores of members of any group should be described (essential).

(6) Sample description.
A description of how the research sample was identified and selected should be included (essential). The race, sex, and ethnic composition of the sample, including those groups set forth in section 4A above, should be described (essential). This description should include the size of each subgroup (essential). A description of how the research sample compares with the relevant labor market or work force, the method by which the relevant labor market or work force was defined, and a discussion of the likely effects on validity of differences between the sample and the relevant labor market or work force, are also desirable. Descriptions of educational levels, length of service, and age are also desirable.

(7) Description of selection procedures.
Any measure, combination of measures, or procedure studied should be completely and explicitly described or attached (essential). If commercially available selection procedures are studied, they should be described by title, form, and publisher (essential). Reports of reliability estimates and how they were established are desirable.

(8) Techniques and results.
Methods used in analyzing data should be described (essential). Measures of central tendency (e.g., means) and measures of dispersion (e.g., standard deviations and ranges) for all selection procedures and all criteria should be reported for each race, sex, and ethnic group which constitutes a significant factor in the relevant labor market (essential). The magnitude and direction of all relationships between selection procedures and criterion measures investigated should be reported for each relevant race, sex, and ethnic group and for the total group (essential). Where groups are too small to obtain reliable evidence of the magnitude of the relationship, need not be reported separately. Statements regarding the statistical significance of results should be made (essential). Any statistical adjustments, such as for less than perfect reliability or for restriction of score range in the selection procedure or criterion should be described and explained; and uncorrected correlation coefficients should also be shown (essential). Where the statistical technique categorizes continuous data, such as biserial correlation and the phi coefficient, the categories and the bases on which they were determined should be described and explained (essential). Studies of test fairness should be included where called for by the requirements of section 14B(8) (essential). These studies should include the rationale by which a selection procedure was determined to be fair to the group(s) in question. Where test fairness or unfairness has been demonstrated on the basis of other studies, a bibliography of the relevant studies should be included (essential). If the bibliography includes unpublished studies, copies of these studies, or adequate abstracts or summaries, should be attached (essential). Where revisions have been made in a selection procedure to assure compatibility between successful job performance and the probability of being selected, the studies underlying such revisions should be included (essential). All statistical results should be organized and presented by relevant race, sex, and ethnic group (essential).
(9) Alternative procedures investigated.
The selection procedures investigated and available evidence of their impact should be identified (essential). The scope, method, and findings of the investigation, and the conclusions reached in light of the findings, should be fully described (essential).

(10) Uses and applications.
The methods considered for use of the selection procedure (e.g., as a screening device with a cutoff score, for grouping or ranking, or combined with other procedures in a battery) and available evidence of their impact should be described (essential). This description should include the rationale for choosing the method for operational use, and the evidence of the validity and utility of the procedure as it is to be used (essential). The purpose for which the procedure is to be used (e.g., hiring, transfer, promotion) should be described (essential). If weights are assigned to different parts of the selection procedure, these weights and the validity of the weighted composite should be reported (essential). If the selection procedure is used with a cutoff score, the user should describe the way in which normal expectations of proficiency within the work force were determined and the way in which the cutoff score was determined (essential).

(11) Source data.
Each user should maintain records showing all pertinent information about individual sample members and raters where they are used, in studies involving the validation of selection procedures. These records should be made available upon request of a compliance agency. In the case of individual sample members these data should include scores on the selection procedure(s), scores on criterion measures, age, sex, race, or ethnic group status, and experience on the specific job on which the validation study was conducted, and may also include such things as education, training, and prior job experience, but should not include names and social security numbers. Records should be maintained which show the ratings given to each sample member by each rater.

(12) Contact person.
The name, mailing address, and telephone number of the person who may be contacted for further information about the validity study should be provided (essential).

(13) Accuracy and completeness.
The report should describe the steps taken to assure the accuracy and completeness of the collection, analysis, and report of data and results.

C. Content validity studies.
Reports of content validity for a selection procedure should include the following information:
(1) User(s), location(s) and date(s) of study. Dates and location(s) of the job analysis should be shown (essential).

(2) Problem and setting. An explicit definition of the purpose(s) of the study and the circumstances in which the study was conducted should be provided. A description of existing selection procedures and cutoff scores, if any, should be provided.

(3) Job analysis—Content of the job. A description of the method used to analyze the job should be provided (essential). The work behavior(s), the associated tasks, and, if the behavior results in a work product, the work products should be completely described (essential). Measures of criticality and/or importance of the work behavior(s) and the method of determining these measures should be provided (essential). Where the job analysis also identified the knowledges, skills, and abilities used in work behavior(s), an operational definition for each knowledge in terms of a body of learned information and for each skill and ability in terms of observable behaviors and outcomes, and the relationship between each knowledge, skill, or ability and each work behavior, as well as the method used to determine this relationship, should be provided (essential). The work situation should be described, including the setting in which work behavior(s) are performed, and where appropriate, the manner in which knowledges, skills, or abilities are used, and the complexity and difficulty of the knowledge, skill, or ability as used in the work behavior(s).

(4) Selection procedure and its content. Selection procedures, including those constructed by or for the user, specific training requirements, composites of selection procedures, and any other procedure supported by content validity, should be completely and explicitly described or attached (essential). If commercially available selection procedures are used, they should be described by title, form, and publisher (essential). The behaviors measured or sampled by the selection procedure should be explicitly described (essential). Where the selection procedure purports to measure a knowledge, skill, or ability, evidence that the selection procedure measures and is a representative sample of the knowledge, skill, or ability should be provided (essential).

(5) Relationship between the selection procedure and the job. The evidence demonstrating that the selection procedure is a representative work sample, a representative sample of the work behavior(s), or a representative sample of a knowledge, skill, or ability as used as a part of a work behavior and necessary for that behavior should be provided (essential). The user should identify the work behavior(s) which each item or part of the selection procedure is intended to sample or measure (essential). Where the selection procedure purports to sample a work behavior or to provide a sample of a work product, a comparison should be provided of the manner, setting, and the level of
complexity of the selection procedure with those of the work situation (essential). If any steps were taken to reduce adverse impact on a race, sex, or ethnic group in the content of the procedure or in its administration, these steps should be described. Establishment of time limits, if any, and how these limits are related to the speed with which duties must be performed on the job, should be explained. Measures of central tendency (e.g., means) and measures of dispersion (e.g., standard deviations) and estimates of reliability should be reported for all selection procedures if available. Such reports should be made for relevant race, sex, and ethnic subgroups, at least on a statistically reliable sample basis.

(6) Alternative procedures investigated.
The alternative selection procedures investigated and available evidence of their impact should be identified (essential). The scope, method, and findings of the investigation, and the conclusions reached in light of the findings, should be fully described (essential).

(7) Uses and applications.
The methods considered for use of the selection procedure (e.g., as a screening device with a cutoff score, for grouping or ranking, or combined with other procedures in a battery) and available evidence of their impact should be described (essential). This description should include the rationale for choosing the method for operational use, and the evidence of the validity and utility of the procedure as it is to be used (essential). The purpose for which the procedure is to be used (e.g., hiring, transfer, promotion) should be described (essential). If the selection procedure is used with a cutoff score, the user should describe the way in which normal expectations of proficiency within the work force were determined and the way in which the cutoff score was determined (essential). In addition, if the selection procedure is to be used for ranking, the user should specify the evidence showing that a higher score on the selection procedure is likely to result in better job performance.

(8) Contact person.
The name, mailing address, and telephone number of the person who may be contacted for further information about the validity study should be provided (essential).

(9) Accuracy and completeness.
The report should describe the steps taken to assure the accuracy and completeness of the collection, analysis, and report of data and results.

D. Construct validity studies.
Reports of construct validity for a selection procedure should include the following information:

(1) User(s), location(s), and date(s) of study.
Date(s) and location(s) of the job analysis and the gathering of other evidence called for by these guidelines should be provided (essential).

(2) Problem and setting.
An explicit definition of the purpose(s) of the study and the circumstances in which the study was conducted should be provided. A description of existing selection procedures and cutoff scores, if any, should be provided.

(3) Construct definition.
A clear definition of the construct(s) which are believed to underlie successful performance of the critical or important work behavior(s) should be provided (essential). This definition should include the levels of construct performance relevant to the job(s) for which the selection procedure is to be used (essential). There should be a summary of the position of the construct in the psychological literature, or in the absence of such a position, a description of the way in which the definition and measurement of the construct was developed and the psychological theory underlying it (essential). Any quantitative data which identify or define the job constructs, such as factor analyses, should be provided (essential).

(4) Job analysis.
A description of the method used to analyze the job should be provided (essential). A complete description of the work behavior(s) and, to the extent appropriate, work outcomes and measures of their criticality and/or importance should be provided (essential). The report should also describe the basis on which the behavior(s) or outcomes were determined to be important, such as their level of difficulty, their frequency of performance, the consequences of error or other appropriate factors (essential). Where jobs are grouped or compared for the purposes of generalizing validity evidence, the work behavior(s) and work product(s) for each of the jobs should be described, and conclusions concerning the similarity of the jobs in terms of observable work behaviors or work products should be made (essential).

(5) Job titles and codes.
It is desirable to provide the selection procedure user's job title(s) for the job(s) in question and the corresponding job title(s) and code(s) from the United States Employment Service's dictionary of occupational titles.

(6) Selection procedure.
The selection procedure used as a measure of the construct should be completely and explicitly described or attached (essential). If commercially available selection procedures are used, they should be identified by title, form and publisher (essential). The research evidence of the relationship between the selection procedure and the construct, such as factor structure, should be included (essential). Measures of central tendency, variability and reliability of the selection procedure should be provided (essential). Whenever feasible, these
measures should be provided separately for each relevant race, sex and ethnic group.

(7) Relationship to job performance.
The criterion-related study(ies) and other empirical evidence of the relationship between the construct measured by the selection procedure and the related work behavior(s) for the job or jobs in question should be provided (essential). Documentation of the criterion-related study(ies) should satisfy the provisions of section 15B above or section 15E(1) below, except for studies conducted prior to the effective date of these guidelines (essential). Where a study pertains to a group of jobs, and, on the basis of the study, validity is asserted for a job in the group, the observed work behaviors and the observed work products for each of the jobs should be described (essential). Any other evidence used in determining whether the work behavior(s) in each of the jobs is the same should be fully described (essential).

(8) Alternative procedures investigated.
The alternative selection procedures investigated and available evidence of their impact should be identified (essential). The scope, method, and findings of the investigation, and the conclusions reached in light of the findings should be fully described (essential).

(9) Uses and applications.
The methods considered for use of the selection procedure (e.g., as a screening device with a cutoff score, for grouping or ranking, or combined with other procedures in a battery) and available evidence of their impact should be described (essential). This description should include the rationale for choosing the method for operational use, and the evidence of the validity and utility of the procedure as it is to be used (essential). The purpose for which the procedure is to be used (e.g., hiring, transfer, promotion) should be described (essential). If weights are assigned to different parts of the selection procedure, these weights and the validity of the weighted composite should be reported (essential). If the selection procedure is used with a cutoff score, the user should describe the way in which normal expectations of proficiency within the work force were determined and the way in which the cutoff score was determined (essential).

(10) Accuracy and completeness.
The report should describe the steps taken to assure the accuracy and completeness of the collection, analysis, and report of data and results.

(11) Source data.
Each user should maintain records showing all pertinent information relating to its study of construct validity.

(12) Contact person.
The name, mailing address, and telephone number of the individual who may be contacted for further information about the validity study should be provided (essential).

E. Evidence of validity from other studies.
When validity of a selection procedure is supported by studies not done by the user, the evidence from the original study or studies should be compiled in a manner similar to that required in the appropriate section of this section 15 above. In addition, the following evidence should be supplied:

(1) Evidence from criterion-related validity studies
   A description of the important job behavior(s) of the user's job and the basis on which the behaviors were determined to be important should be provided (essential). A full description of the basis for determining that these important work behaviors are the same as those of the job in the original study (or studies) should be provided (essential).

   b. Relevance of criteria.
   A full description of the basis on which the criteria used in the original studies are determined to be relevant for the user should be provided (essential).

   c. Other variables.
   The similarity of important applicant pool or sample characteristics reported in the original studies to those of the user should be described (essential). A description of the comparison between the race, sex and ethnic composition of the user’s relevant labor market and the sample in the original validity studies should be provided (essential).

   d. Use of the selection procedure.
   A full description should be provided showing that the use to be made of the selection procedure is consistent with the findings of the original validity studies (essential).

   e. Bibliography.
   A bibliography of reports of validity of the selection procedure for the job or jobs in question should be provided (essential). Where any of the studies included an investigation of test fairness, the results of this investigation should be provided (essential). Copies of reports published in journals that are not commonly available should be described in detail or attached (essential). Where a user is relying upon unpublished studies, a reasonable effort should be made to obtain these studies. If these unpublished studies are the sole source of validity evidence they should be described in detail or attached (essential). If these studies are not available, the name and address of the source, an adequate abstract or summary of the validity study and data, and a contact person in the source organization should be provided (essential).
(2) Evidence from content validity studies.
See section 14C(3) and section 15C above.

(3) Evidence from construct validity studies.
See sections 14D(2) and 15D above.

F. Evidence of validity from cooperative studies.
Where a selection procedure has been validated through a cooperative study, evidence that the study satisfies the requirements of sections 7, 8 and 15E should be provided (essential).

G. Selection for higher level job.
If a selection procedure is used to evaluate candidates for jobs at a higher level than those for which they will initially be employed, the validity evidence should satisfy the documentation provisions of this section 15 for the higher level job or jobs, and in addition, the user should provide: (1) A description of the job progression structure, formal or informal; (2) the data showing how many employees progress to the higher level job and the length of time needed to make this progression; and (3) an identification of any anticipated changes in the higher level job. In addition, if the test measures a knowledge, skill or ability, the user should provide evidence that the knowledge, skill or ability is required for the higher level job and the basis for the conclusion that the knowledge, skill or ability is not expected to develop from the training or experience on the job.

H. Interim use of selection procedures.
If a selection procedure is being used on an interim basis because the procedure is not fully supported by the required evidence of validity, the user should maintain and have available (1) substantial evidence of validity for the procedure, and (2) a report showing the date on which the study to gather the additional evidence commenced, the estimated completion date of the study, and a description of the data to be collected (essential).

Definitions
Sec. 16. Definitions.
The following definitions shall apply throughout these guidelines:

A. Ability.
A present competence to perform an observable behavior or a behavior which results in an observable product.

B. Adverse impact.
A substantially different rate of selection in hiring, promotion, or other employment decision which works to the disadvantage of members of a race, sex, or ethnic group. See section 4 of these guidelines.
C. Compliance with these guidelines.
Use of a selection procedure is in compliance with these guidelines if such use has been validated in accord with these guidelines (as defined below), or if such use does not result in adverse impact on any race, sex, or ethnic group (see section 4, above), or, in unusual circumstances, if use of the procedure is otherwise justified in accord with Federal law. See section 6B, above.

D. Content validity.
Demonstrated by data showing that the content of a selection procedure is representative of important aspects of performance on the job. See section 5B and section 14C.

E. Construct validity.
Demonstrated by data showing that the selection procedure measures the degree to which candidates have identifiable characteristics which have been determined to be important for successful job performance. See section 5B and section 14D.

F. Criterion-related validity.
Demonstrated by empirical data showing that the selection procedure is predictive of or significantly correlated with important elements of work behavior. See sections 5B and 14B.

G. Employer.
Any employer subject to the provisions of the Civil Rights Act of 1964, as amended, including State or local governments and any Federal agency subject to the provisions of section 717 of the Civil Rights Act of 1964, as amended, and any Federal contractor or subcontractor or federally assisted construction contractor or subcontractor covered by Executive Order 11246, as amended.

H. Employment agency.
Any employment agency subject to the provisions of the Civil Rights Act of 1964, as amended.

I. Enforcement action.
For the purposes of section 4 a proceeding by a Federal enforcement agency such as a lawsuit or an administrative proceeding leading to debarment from or withholding, suspension, or termination of Federal Government contracts or the suspension or withholding of Federal Government funds; but not a finding of reasonable cause or a conciliation process or the issuance of right to sue letters under title VII or under Executive Order 11246 where such finding, conciliation, or issuance of notice of right to sue is based upon an individual complaint.

J. Enforcement agency.
Any agency of the executive branch of the Federal Government which adopts these guidelines for purposes of the enforcement of the equal employment opportunity laws or which has responsibility for securing compliance with them.

K. Job analysis.
A detailed statement of work behaviors and other information relevant to the job.

L. Job description.
A general statement of job duties and responsibilities.

M. Knowledge.
A body of information applied directly to the performance of a function.

N. Labor organization.
Any labor organization subject to the provisions of the Civil Rights Act of 1964, as amended, and any committee subject thereto controlling apprenticeship or other training.

O. Observable.
Able to be seen, heard, or otherwise perceived by a person other than the person performing the action.

P. Race, sex, or ethnic group.
Any group of persons identifiable on the grounds of race, color, religion, sex, or national origin.

Q. Selection procedure.
Any measure, combination of measures, or procedure used as a basis for any employment decision. Selection procedures include the full range of assessment techniques from traditional paper and pencil tests, performance tests, training programs, or probationary periods and physical, educational, and work experience requirements through informal or casual interviews and unscored application forms.

R. Selection rate.
The proportion of applicants or candidates who are hired, promoted, or otherwise selected.

S. Should.
The term “should” as used in these guidelines is intended to connote action which is necessary to achieve compliance with the guidelines, while recognizing that there are circumstances where alternative courses of action are open to users.

T. Skill.
A present, observable competence to perform a learned psychomotor act.
U. Technical feasibility.
The existence of conditions permitting the conduct of meaningful criterion-related validity studies. These conditions include: (1) An adequate sample of persons available for the study to achieve findings of statistical significance; (2) having or being able to obtain a sufficient range of scores on the selection procedure and job performance measures to produce validity results which can be expected to be representative of the results if the ranges normally expected were utilized; and (3) having or being able to devise unbiased, reliable and relevant measures of job performance or other criteria of employee adequacy. See section 14B(2). With respect to investigation of possible unfairness, the same considerations are applicable to each group for which the study is made. See section 14B(8).

V. Unfairness of selection procedure.
A condition in which members of one race, sex, or ethnic group characteristically obtain lower scores on a selection procedure than members of another group, and the differences are not reflected in differences in measures of job performance. See section 14B(7).

W. User.
Any employer, labor organization, employment agency, or licensing or certification board, to the extent it may be covered by Federal equal employment opportunity law, which uses a selection procedure as a basis for any employment decision. Whenever an employer, labor organization, or employment agency is required by law to restrict recruitment for any occupation to those applicants who have met licensing or certification requirements, the licensing or certifying authority to the extent it may be covered by Federal equal employment opportunity law will be considered the user with respect to those licensing or certification requirements. Whenever a State employment agency or service does no more than administer or monitor a procedure as permitted by Department of Labor regulations, and does so without making referrals or taking any other action on the basis of the results, the State employment agency will not be deemed to be a user.

X. Validated in accord with these guidelines or properly validated.
A demonstration that one or more validity study or studies meeting the standards of these guidelines has been conducted, including investigation and, where appropriate, use of suitable alternative selection procedures as contemplated by section 3B, and has produced evidence of validity sufficient to warrant use of the procedure for the intended purpose under the standards of these guidelines.

Y. Work behavior.
An activity performed to achieve the objectives of the job. Work behaviors involve observable (physical) components and unobservable (mental) components. A work behavior consists of the performance of one or more tasks. Knowledges,
skills, and abilities are not behaviors, although they may be applied in work behaviors.

Appendix

17. Policy statement on affirmative action
(see section 13B). The Equal Employment Opportunity Coordinating Council was established by act of Congress in 1972, and charged with responsibility for developing and implementing agreements and policies designed, among other things, to eliminate conflict and inconsistency among the agencies of the Federal Government responsible for administering Federal law prohibiting discrimination on grounds of race, color, sex, religion, and national origin. This statement is issued as an initial response to the requests of a number of State and local officials for clarification of the Government’s policies concerning the role of affirmative action in the overall equal employment opportunity program. While the Coordinating Council’s adoption of this statement expresses only the views of the signatory agencies concerning this important subject, the principles set forth below should serve as policy guidance for other Federal agencies as well.

(1) Equal employment opportunity is the law of the land. In the public sector of our society this means that all persons, regardless of race, color, religion, sex, or national origin shall have equal access to positions in the public service limited only by their ability to do the job. There is ample evidence in all sectors of our society that such equal access frequently has been denied to members of certain groups because of their sex, racial, or ethnic characteristics. The remedy for such past and present discrimination is twofold.

On the one hand, vigorous enforcement of the laws against discrimination is essential. But equally, and perhaps even more important are affirmative, voluntary efforts on the part of public employers to assure that positions in the public service are genuinely and equally accessible to qualified persons, without regard to their sex, racial, or ethnic characteristics. Without such efforts equal employment opportunity is no more than a wish. The importance of voluntary affirmative action on the part of employers is underscored by title VII of the Civil Rights Act of 1964, Executive Order 11246, and related laws and regulations—all of which emphasize voluntary action to achieve equal employment opportunity.

As with most management objectives, a systematic plan based on sound organizational analysis and problem identification is crucial to the accomplishment of affirmative action objectives. For this reason, the Council urges all State and local governments to develop and implement results oriented affirmative action plans which deal with the problems so identified.

The following paragraphs are intended to assist State and local governments by illustrating the kinds of analyses and activities which may be appropriate for a public employer's voluntary affirmative action plan. This statement does not address remedies imposed after a finding of unlawful discrimination.
(2) Voluntary affirmative action to assure equal employment opportunity is appropriate at any stage of the employment process. The first step in the construction of any affirmative action plan should be an analysis of the employer’s work force to determine whether percentages of sex, race, or ethnic groups in individual job classifications are substantially similar to the percentages of those groups available in the relevant job market who possess the basic job-related qualifications.

When substantial disparities are found through such analyses, each element of the overall selection process should be examined to determine which elements operate to exclude persons on the basis of sex, race, or ethnic group. Such elements include, but are not limited to, recruitment, testing, ranking certification, interview, recommendations for selection, hiring, promotion, etc. The examination of each element of the selection process should at a minimum include a determination of its validity in predicting job performance.

(3) When an employer has reason to believe that its selection procedures have the exclusionary effect described in paragraph 2 above, it should initiate affirmative steps to remedy the situation. Such steps, which in design and execution may be race, color, sex, or ethnic “conscious,” include, but are not limited to, the following:

(a) The establishment of a long-term goal, and short-range, interim goals and timetables for the specific job classifications, all of which should take into account the availability of basically qualified persons in the relevant job market;

(b) A recruitment program designed to attract qualified members of the group in question;

(c) A systematic effort to organize work and redesign jobs in ways that provide opportunities for persons lacking “journeyman” level knowledge or skills to enter and, with appropriate training, to progress in a career field;

(d) Revamping selection instruments or procedures which have not yet been validated in order to reduce or eliminate exclusionary effects on particular groups in particular job classifications;

(e) The initiation of measures designed to assure that members of the affected group who are qualified to perform the job are included within the pool of persons from which the selecting official makes the selection;

(f) A systematic effort to provide career advancement training, both classroom and on-the-job, to employees locked into dead end jobs; and
(g) The establishment of a system for regularly monitoring the effectiveness of
the particular affirmative action program, and procedures for making timely
adjustments in this program where effectiveness is not demonstrated.

(4) The goal of any affirmative action plan should be achievement of
genuine equal employment opportunity for all qualified persons. Selection under
such plans should be based upon the ability of the applicant(s) to do the work.
Such plans should not require the selection of the unqualified, or the unneeded,
nor should they require the selection of persons on the basis of race, color, sex,
religion, or national origin. Moreover, while the Council believes that this
statement should serve to assist State and local employers, as well as Federal
agencies, it recognizes that affirmative action cannot be viewed as a standardized
program which must be accomplished in the same way at all times in all places.

Accordingly, the Council has not attempted to set forth here either the minimum
or maximum voluntary steps that employers may take to deal with their
respective situations. Rather, the Council recognizes that under applicable
authorities, State and local employers have flexibility to formulate affirmative
action plans that are best suited to their particular situations. In this manner, the
Council believes that affirmative action programs will best serve the goal of equal
employment opportunity.

Respectfully submitted,

Harold R. Tyler, Jr.,
Deputy Attorney General and Chairman of the Equal Employment
Coordinating Council.

Michael H. Moskow,
Under Secretary of Labor.

Ethel Bent Walsh,

Robert E. Hampton,
Chairman, Civil Service Commission.

Arthur E. Flemming,
Chairman, Commission on Civil Rights.
Because of its equal employment opportunity responsibilities under the State and Local Government Fiscal Assistance Act of 1972 (the revenue sharing act), the Department of Treasury was invited to participate in the formulation of this policy statement; and it concurs and joins in the adoption of this policy statement.

Done this 26th day of August 1976.

Richard Albrecht,
General Counsel, Department of the Treasury.

Section 18. Citations.
The official title of these guidelines is “Uniform Guidelines on Employee Selection Procedures (1978)”. The Uniform Guidelines on Employee Selection Procedures (1978) are intended to establish a uniform Federal position in the area of prohibiting discrimination in employment practices on grounds of race, color, religion, sex, or national origin. These guidelines have been adopted by the Equal Employment Opportunity Commission, the Department of Labor, the Department of Justice, and the Civil Service Commission.

The official citation is:


The short form citation is:


When the guidelines are cited in connection with the activities of one of the issuing agencies, a specific citation to the regulations of that agency can be added at the end of the above citation. The specific additional citations are as follows:

Equal Employment Opportunity Commission

29 CFR Part 1607

Department of Labor

Office of Federal Contract Compliance Programs

41 CFR Part 60-3
Department of Justice

28 CFR 50.14

Civil Service Commission

5 CFR 300.103(c)

Normally when citing these guidelines, the section number immediately preceding the title of the guidelines will be from these guidelines series 1-18. If a section number from the codification for an individual agency is needed it can also be added at the end of the agency citation. For example, section 6A of these guidelines could be cited for EEOC as follows: “Section 6A, Uniform Guidelines on Employee Selection Procedures (1978); 43 FR ____, (August 25, 1978); 29 CFR part 1607, section 6A.”

Eleanor Holmes Norton,
Chair, Equal Employment Opportunity Commission.

Alan K. Campbell,
Chairman, Civil Service Commission.

Ray Marshall,
Secretary of Labor.

Griffin B. Bell,
Attorney General.

Official Citation:

28 CFR Section 50.15: Representation of Federal officials and employees by Department of Justice attorneys or by private counsel furnished by the Department in civil, criminal, and congressional proceedings in which Federal employees are sued, subpoenaed, or charged in their individual capacities.
(a) Under the procedures set forth below, a federal employee (hereby defined to include present and former Federal officials and employees) may be provided representation in civil, criminal and Congressional proceedings in which he is sued, subpoenaed, or charged in his individual capacity, not covered by § 15.1 of this chapter, when the actions for which representation is requested reasonably appear to have been performed within the scope of the employee's employment and the Attorney General or his designee determines that providing representation would otherwise be in the interest of the United States. No special form of request for representation is required when it is clear from the proceedings in a case that the employee is being sued solely in his official capacity and only equitable relief is sought. (See USAM 4-13.000)

(1) When an employee believes he is entitled to representation by the Department of Justice in a proceeding, he must submit forthwith a written request for that representation, together with all process and pleadings served upon him, to his immediate supervisor or whomever is designated by the head of his department or agency. Unless the employee's employing federal agency concludes that representation is clearly unwarranted, it shall submit, in a timely manner, to the Civil Division or other appropriate litigating division (Antitrust, Civil Rights, Criminal, Land and Natural Resources or the Tax Division), a statement containing its findings as to whether the employee was acting within the scope of his employment and its recommendation for or against providing representation. The statement should be accompanied by all available factual information. In emergency situations the litigating division may initiate conditional representation after a telephone request from the appropriate official of the employing agency. In such cases, the written request and appropriate documentation must be subsequently provided.

(2) Upon receipt of the individual's request for counsel, the litigating division shall determine whether the employee's actions reasonably appear to have been performed within the scope of his employment and whether providing representation would be in the interest of the United States. In circumstances where considerations of professional ethics prohibit direct review of the facts by attorneys of the litigating division (e.g. because of the possible existence of interdefendant conflicts) the litigating division may delegate the fact-finding aspects of this function to other components of the Department or to a private attorney at federal expenses.

(3) Attorneys employed by any component of the Department of Justice who participate in any process utilized for the purpose of determining whether the Department should provide representation to a federal employee, undertake a full and traditional attorney-client relationship with the employee with respect to application of the attorney-client privilege. If representation is authorized, Justice Department attorneys who represent an employee under this section also undertake a full and traditional attorney-client relationship with the employee.
with respect to the attorney-client privilege. Any adverse information communicated by the client-employee to an attorney during the course of such attorney-client relationship shall not be disclosed to anyone, either inside or outside the Department, other than attorneys responsible for representation of the employee, unless such disclosure is authorized by the employee. Such adverse information shall continue to be fully protected whether or not representation is provided, and even though representation may be denied or discontinued. The extent, if any, to which attorneys employed by an agency other than the Department of Justice undertake a full and traditional attorney-client relationship with the employee with respect to the attorney-client privilege, either for purposes of determining whether representation should be provided or to assist Justice Department attorneys in representing the employee, shall be determined by the agency employing the attorneys.

(4) Representation generally is not available in federal criminal proceedings. Representation may be provided to a federal employee in connection with a federal criminal proceeding only where the Attorney General or his designee determines that representation is in the interest of the United States and subject to applicable limitations of § 50.16. In determining whether representation in a federal criminal proceeding is in the interest of the United States, the Attorney General or his designee shall consider, among other factors, the relevance of any non-prosecutorial interests of the United States, the importance of the interests implicated, the Department's ability to protect those interests through other means, and the likelihood of a conflict of interest between the Department's prosecutorial and representational responsibilities. If representation is authorized, the Attorney General or his designee also may determine whether representation by Department attorneys, retention of private counsel at federal expense, or reimbursement to the employee of private counsel fees is most appropriate under the circumstances.

(5) Where representation is sought for proceedings other than federal criminal proceedings, but there appears to exist the possibility of a federal criminal investigation or indictment relating to the same subject matter, the litigating division shall contact a designated official in the Criminal, Civil Rights or Tax Division or other prosecutive authority within the Department (hereinafter “prosecuting division”) to determine whether the employee is either a subject of a federal criminal investigation or a defendant in a federal criminal case. An employee is the subject of an investigation if, in addition to being circumstantially implicated by having the appropriate responsibilities at the appropriate time, there is some evidence of his specific participation in a crime.

(6) If a prosecuting division of the Department indicates that the employee is not the subject of a criminal investigation concerning the act or acts for which he seeks representation, then representation may be provided if otherwise permissible under the provisions of this section. Similarly, if the prosecuting division indicates that there is an ongoing investigation, but into a matter
unrelated to that for which representation has been requested, then representation may be provided.

(7) If the prosecuting division indicates that the employee is the subject of a federal criminal investigation concerning the act or acts for which he seeks representation, the litigating division shall inform the employee that no representation by Justice Department attorneys will be provided in that federal criminal proceeding or in any related civil, congressional, or state criminal proceeding. In such a case, however, the litigating division, in its discretion, may provide a private attorney to the employee at federal expense under the procedures of § 50.16, or provide reimbursement to employees for private attorney fees incurred in connection with such related civil, congressional, or state criminal proceeding, provided no decision has been made to seek an indictment or file an information against the employee.

(8) In any case where it is determined that Department of Justice attorneys will represent a federal employee, the employee must be notified of his right to retain private counsel at his own expense. If he elects representation by Department of Justice attorneys, the employee and his agency shall be promptly informed:

(i) That in actions where the United States, any agency, or any officer thereof in his official capacity is also named as a defendant, the Department of Justice is required by law to represent the United States and/or such agency or officer and will assert all appropriate legal positions and defenses on behalf of such agency, officer and/or the United States;

(ii) That the Department of Justice will not assert any legal position or defense on behalf of any employee sued in his individual capacity which is deemed not to be in the interest of the United States;

(iii) Where appropriate, that neither the Department of Justice nor any agency of the U.S. Government is obligated to pay or to indemnify the defendant employee for any judgment for money damages which may be rendered against such employee; but that, where authorized, the employee may apply for such indemnification from his employing agency upon the entry of an adverse verdict, judgment, or other monetary award;

(iv) That any appeal by Department of Justice attorneys from an adverse ruling or judgment against the employee may only be taken upon the discretionary approval of the Solicitor General, but the employee-defendant may pursue an appeal at his own expense whenever the Solicitor General declines to authorize an appeal and private counsel is not provided at federal expense under the procedures of § 50.16; and
(v) That while no conflict appears to exist at the time representation is tendered which would preclude making all arguments necessary to the adequate defense of the employee, if such conflict should arise in the future the employee will be promptly advised and steps will be taken to resolve the conflict as indicated by paragraph (a) (6), (9) and (10) of this section, and by § 50.16.

(9) If a determination not to provide representation is made, the litigating division shall inform the agency and/or the employee of the determination.

(10) If conflicts exist between the legal and factual positions of various employees in the same case which make it inappropriate for a single attorney to represent them all, the employees may be separated into as many compatible groups as is necessary to resolve the conflict problem and each group may be provided with separate representation. Circumstances may make it advisable that private representation be provided to all conflicting groups and that direct Justice Department representation be withheld so as not to prejudice particular defendants. In such situations, the procedures of § 50.16 will apply.

(11) Whenever the Solicitor General declines to authorize further appellate review or the Department attorney assigned to represent an employee becomes aware that the representation of the employee could involve the assertion of a position that conflicts with the interests of the United States, the attorney shall fully advise the employee of the decision not to appeal or the nature, extent, and potential consequences of the conflict. The attorney shall also determine, after consultation with his supervisor (and, if appropriate, with the litigating division) whether the assertion of the position or appellate review is necessary to the adequate representation of the employee and

(i) If it is determined that the assertion of the position or appeal is not necessary to the adequate representation of the employee, and if the employee knowingly agrees to forego appeal or to waive the assertion of that position, governmental representation may be provided or continued; or

(ii) If the employee does not consent to forego appeal or waive the assertion of the position, or if it is determined that an appeal or assertion of the position is necessary to the adequate representation of the employee, a Justice Department lawyer may not provide or continue to provide the representation; and

(iii) In appropriate cases arising under paragraph (a)(10)(ii) of this section, a private attorney may be provided at federal expense under the procedures of § 50.16.

(12) Once undertaken, representation of a federal employee under this subsection will continue until either all appropriate proceedings, including
applicable appellate procedures approved by the Solicitor General, have ended, or until any of the bases for declining or withdrawing from representation set forth in this section is found to exist, including without limitation the basis that representation is not in the interest of the United States. If representation is discontinued for any reason, the representing Department attorney on the case will seek to withdraw but will take all reasonable steps to avoid prejudice to the employee.

(b) Representation is not available to a federal employee whenever:

(1) The conduct with regard to which the employee desires representation does not reasonably appear to have been performed within the scope of his employment with the federal government;

(2) It is otherwise determined by the Department that it is not in the interest of the United States to provide representation to the employee.

(c)(1) The Department of Justice may indemnify the defendant Department of Justice employee for any verdict, judgment, or other monetary award which is rendered against such employee, provided that the conduct giving rise to the verdict, judgment, or award was taken within the scope of employment and that such indemnification is in the interest of the United States, as determined by the Attorney General or his designee.

(2) The Department of Justice may settle or compromise a personal damages claim against a Department of Justice employee by the payment of available funds, at any time, provided the alleged conduct giving rise to the personal damages claim was taken within the scope of employment and that such settlement or compromise is in the interest of the United States, as determined by the Attorney General or his designee.

(3) Absent exceptional circumstances as determined by the Attorney General or his designee, the Department will not entertain a request either to agree to indemnify or to settle a personal damages claim before entry of an adverse verdict, judgment, or award.

(4) The Department of Justice employee may request indemnification to satisfy a verdict, judgment, or award entered against the employee. The employee shall submit a written request, with appropriate documentation including copies of the verdict, judgment, award, or settlement proposal if on appeal, to the head of his employing component, who shall thereupon submit to the appropriate Assistant Attorney General, in a timely manner, a recommended disposition of the request. Where appropriate, the Assistant Attorney General shall seek the views of the U.S. Attorney; in all such cases the Civil Division shall be consulted. The Assistant Attorney General shall forward the request, the employing
component's recommendation, and the Assistant Attorney General's recommendation to the Attorney General for decision.

(5) Any payment under this section either to indemnify a Department of Justice employee or to settle a personal damages claim shall be contingent upon the availability of appropriated funds of the employing component of the Department of Justice.

Official Citation:

28 CFR Section 50.16: Representation of Federal employees by private counsel at Federal expense.

(a) Representation by private counsel at federal expense or reimbursement of private counsel fees is subject to the availability of funds and may be provided to a federal employee only in the instances described in § 50.15(a) (4), (7), (10), and (11), and in appropriate circumstances, for the purposes set forth in § 50.15(a)(2).

(b) To ensure uniformity in retention and reimbursement procedures among the litigating divisions, the Civil Division shall be responsible for establishing procedures for the retention of private counsel and the reimbursement to an employee of private counsel fees, including the setting of fee schedules. In all instances where a litigating division decides to retain private counsel or to provide reimbursement of private counsel fees under this section, the Civil Division shall be consulted before the retention or reimbursement is undertaken.

(c) Where private counsel is provided, the following procedures shall apply:

(1) While the Department of Justice will generally defer to the employee's choice of counsel, the Department must approve in advance any private counsel to be retained under this section. Where national security interests may be involved, the Department of Justice will consult with the agency employing the federal defendant seeking representation.

(2) Federal payments to private counsel for an employee will cease if the private counsel violates any of the terms of the retention agreement or the Department of Justice.

(i) Decides to seek an indictment of, or to file an information against, that employee on a federal criminal charge relating to the conduct concerning which representation was undertaken;
(ii) Determines that the employee's actions do not reasonably appear to have been performed within the scope of his employment;

(iii) Resolves any conflict described herein and tenders representation by Department of Justice attorneys;

(iv) Determines that continued representation is not in the interest of the United States;

(v) Terminates the retainer with the concurrence of the employee-client for any reason.

(d) Where reimbursement is provided for private counsel fees incurred by employees, the following limitations shall apply:

(1) Reimbursement shall be limited to fees incurred for legal work that is determined to be in the interest of the United States. Reimbursement is not available for legal work that advances only the individual interests of the employee.

(2) Reimbursement shall not be provided if at any time the Attorney General or his designee determines that the employee's actions do not reasonably appear to have been performed within the scope of his employment or that representation is no longer in the interest of the United States.

(3) Reimbursement shall not be provided for fees incurred during any period of time for which representation by Department of Justice attorneys was tendered.

(4) Reimbursement shall not be provided if the United States decides to seek an indictment of or to file an information against the employee seeking reimbursement, on a criminal charge relating to the conduct concerning which representation was undertaken.

**Official Citation:**
[Order No. 970-82, 47 FR 8174, Feb. 25, 1982, as amended by Order No. 1409-90, 55 FR 13130, Apr. 9, 1990]

28 CFR Section 50.17: *Ex parte communications in informal rulemaking proceedings.*

In rulemaking proceedings subject only to the procedural requirements of 5 U.S.C. 553:

Page 742
(a) A general prohibition applicable to all offices, boards, bureaus and divisions of the Department of Justice against the receipt of private, ex parte oral or written communications is undesirable, because it would deprive the Department of the flexibility needed to fashion rulemaking procedures appropriate to the issues involved, and would introduce a degree of formality that would, at least in most instances, result in procedures that are unduly complicated, slow, and expensive, and, at the same time, perhaps not conducive to developing all relevant information.

(b) All written communications from outside the Department addressed to the merits of a proposed rule, received after notice of proposed informal rulemaking and in its course by the Department, its offices, boards, and bureaus, and divisions or their personnel participating in the decision, should be placed promptly in a file available for public inspection.

(c) All oral communications from outside the Department of significant information or argument respecting the merits of a proposed rule, received after notice of proposed informal rulemaking and in its course by the Department, its offices, boards, bureaus, and divisions or their personnel participating in the decision, should be summarized in writing and placed promptly in a file available for public inspection.

(d) The Department may properly withhold from the public files information exempt from disclosure under 5 U.S.C. 552.

(e) The Department may conclude that restrictions on ex parte communications in particular rulemaking proceedings are necessitated by considerations of fairness or for other reasons.

**Official Citation:**

---

28 CFR Section 50.18: [Reserved]

28 CFR Section 50.19: Procedures to be followed by government attorneys prior to filing recusal or disqualification motions.

The determination to seek for any reason the disqualification or recusal of a justice, judge, or magistrate is a most significant and sensitive decision. This is
particularly true for government attorneys, who should be guided by uniform procedures in obtaining the requisite authorization for such a motion. This statement is designed to establish a uniform procedure.

(a) No motion to recuse or disqualify a justice, judge, or magistrate (see, e.g., 28 U.S.C. 144, 455) shall be made or supported by any Department of Justice attorney, U.S. Attorney (including Assistant U.S. Attorneys) or agency counsel conducting litigation pursuant to agreement with or authority delegated by the Attorney General, without the prior written approval of the Assistant Attorney General having ultimate supervisory power over the action in which recusal or disqualification is being considered.

(b) Prior to seeking such approval, Justice Department lawyer(s) handling the litigation shall timely seek the recommendations of the U.S. Attorney for the district in which the matter is pending, and the views of the client agencies, if any. Similarly, if agency attorneys are primarily handling any such suit, they shall seek the recommendations of the U.S. Attorney and provide them to the Department of Justice with the request for approval. In actions where the United States Attorneys are primarily handling the litigation in question, they shall seek the recommendation of the client agencies, if any, for submission to the Assistant Attorney General.

(c) In the event that the conduct and pace of the litigation does not allow sufficient time to seek the prior written approval by the Assistant Attorney General, prior oral authorization shall be sought and a written record fully reflecting that authorization shall be subsequently prepared and submitted to the Assistant Attorney General.

(d) Assistant Attorneys General may delegate the authority to approve or deny requests made pursuant to this section, but only to Deputy Assistant Attorneys General or an equivalent position.

(e) This policy statement does not create or enlarge any legal obligations upon the Department of Justice in civil or criminal litigation, and it is not intended to create any private rights enforceable by private parties in litigation with the United States.

Official Citation:
[Order No. 977-82, 47 FR 22094, May 21, 1982]

28 CFR Section 50.20: Participation by the United States in court-annexed arbitration.
(a) Considerations affecting participation in arbitration.

(1) The Department recognizes and supports the general goals of court-annexed arbitrations, which are to reduce the time and expenses required to dispose of civil litigation. Experimentations with such procedures in appropriate cases can offer both the courts and litigants an opportunity to determine the effectiveness of arbitration as an alternative to traditional civil litigation.

(2) An arbitration system, however, is best suited for the resolution of relatively simple factual issues, not for trying cases that may involve complex issues of liability or other unsettled legal questions. To expand an arbitration system beyond the types of cases for which it is best suited and most competent would risk not only a decrease in the quality of justice available to the parties but unnecessarily higher costs as well.

(3) In particular, litigation involving the United States raises special concerns with respect to court-annexed arbitration programs. A mandatory arbitration program potentially implicates the principles of separation of powers, sovereign immunity, and the Attorney General’s control over the process of settling litigation.

(b) General rule consenting to arbitration consistent with the department’s regulations.

(1) Subject to the considerations set forth in the following paragraphs and the restrictions set forth in paragraphs (c) and (d), in a case assigned to arbitration or mediation under a local district court rule, the Department of Justice agrees to participate in the arbitration process under the local rule. The attorney for the government responsible for the case should take any appropriate steps in conducting the case to protect the interests of the United States.

(2) Based upon its experience under arbitration programs to date, and the purposes and limitations of court-annexed arbitration, the Department generally endorses inclusion in a district’s court-annexed arbitration program of civil actions—

(i) In which the United States or a Department, agency, or official of the United States is a party, and which seek only money damages in an amount not in excess of $100,000, exclusive of interest and costs; and

(ii) Which are brought (A) under the Federal Tort Claims Act, 28 U.S.C. 1346(b), 2671 et seq., or (B) under the Longshoreman’s and Harbor Worker’s Compensation Act, 33 U.S.C. 905, or (C) under the Miller Act, 40 U.S.C. 270(b).
(3) In any other case in which settlement authority has been delegated to the U.S. Attorney under the regulations of the Department and the directives of the applicable litigation division and none of the exceptions to such delegation apply, the U.S. Attorney for the district, if he concludes that a settlement of the case upon the terms of the arbitration award would be appropriate, may proceed to settle the case accordingly.

(4) Cases other than those described in paragraph (2) that are not within the delegated settlement authority of the U.S. Attorney for the district ordinarily are not appropriate for an arbitration process because the Department generally will not be able to act favorably or negatively in a short period of time upon a settlement of the case in accordance with the arbitration award. Therefore, this will result in a demand for trial de novo in a substantial proportion of such cases to preserve the interests of the United States.

(5) The Department recommends that any district court's arbitration rule include a provision exempting any case from arbitration, sua sponte or on motion of a party, in which the objectives of arbitration would not appear to be realized, because the case involves complex or novel legal issues, or because legal issues predominate over factual issues, or for other good cause.

(c) Objection to the imposition of penalties or sanctions against the United States for demanding trial de novo.

(1) Under the principle of sovereign immunity, the United States cannot be held liable for costs or sanctions in litigation in the absence of a statutory provision waiving its immunity. In view of the statutory limitations on the costs payable by the United States (28 U.S.C. 2412(a), 2412(b), and 1920), the Department does not consent to provisions in any district's arbitration program providing for the United States or the Department, agency, or official named as a party to the action to pay any sanction for demanding a trial de novo—either as a deposit in advance or as a penalty imposed after the fact—which is based on the arbitrators' fees, the opposing party's attorneys' fees, or any other costs not authorized by statute to be awarded against the United States. This objection applies whether the penalty or sanction is required to be paid to the opposing party, to the clerk of the court, or to the Treasury of the United States.

(2) In any case involving the United States that is designated for arbitration under a program pursuant to which such a penalty or sanction might be imposed against the United States, its officers or agents, the attorney for the government is instructed to take appropriate steps, by motion, notice of objection, or otherwise, to apprise the court of the objection of the United States to the imposition of such a penalty or sanction.
(3) Should such a penalty or sanction actually be required of or imposed on the United States, its officers or agents, the attorney for the government is instructed to:

(i) Advise the appropriate Assistant Attorney General of this development promptly in writing;

(ii) Seek appropriate relief from the district court; and

(iii) If necessary, seek authority for filing an appeal or petition for mandamus.

The Solicitor General, the Assistant Attorneys General, and the U.S. Attorneys are instructed to take all appropriate steps to resist the imposition of such penalties or sanctions against the United States.

(d) Additional restrictions.

(1) The Assistant Attorneys General, the U.S. Attorneys, and their delegates, have no authority to settle or compromise the interests of the United States in a case pursuant to an arbitration process in any respect that is inconsistent with the limitations upon the delegation of settlement authority under the Department's regulations and the directives of the litigation divisions. See 28 CFR part 0, subpart Y and appendix to subpart Y. The attorney for the government shall demand trial de novo in any case in which:

(i) Settlement of the case on the basis of the amount awarded would not be in the best interests of the United States;

(ii) Approval of a proposed settlement under the Department's regulations in accordance with the arbitration award cannot be obtained within the period allowed by the local rule for rejection of the award; or

(iii) The client agency opposes settlement of the case upon the terms of the settlement award, unless the appropriate official of the Department approves a settlement of the case in accordance with the delegation of settlement authority under the Department’s regulations.

(2) Cases sounding in tort and arising under the Constitution of the United States or under a common law theory filed against an employee of the United States in his personal capacity for actions within the scope of his employment which are alleged to have caused injury or loss of property or personal injury or death are not appropriate for arbitration.

(3) Cases for injunctive or declaratory relief are not appropriate for arbitration.
(4) The Department reserves the right to seek any appropriate relief to which its client is entitled, including injunctive relief or a ruling on motions for judgment on the pleadings, for summary judgment, or for qualified immunity, or on issues of discovery, before proceeding with the arbitration process.

(5) In view of the provisions of the Federal Rules of Evidence with respect to settlement negotiations, the Department objects to the introduction of the arbitration process or the arbitration award in evidence in any proceeding in which the award has been rejected and the case is tried de novo.

(6) The Department's consent for participation in an arbitration program is not a waiver of sovereign immunity or other defenses of the United States except as expressly stated; nor is it intended to affect jurisdictional limitations (e.g., the Tucker Act).

(e) Notification of new or revised arbitration rules.
The U.S. Attorney in a district which is considering the adoption of or has adopted a program of court-annexed arbitration including cases involving the United States shall:

(1) Advise the district court of the provisions of this section and the limitations on the delegation of settlement authority to the United States Attorney pursuant to the Department's regulations and the directives of the litigation divisions; and

(2) Forward to the Executive Office for United States Attorneys a notice that such a program is under consideration or has been adopted, or is being revised, together with a copy of the rules or proposed rules, if available, and a recommendation as to whether United States participation in the program as proposed, adopted, or revised, would be advisable, in whole or in part.

Official Citation:
[Order No. 1109-85, 50 FR 40524, Oct. 4, 1985]

28 CFR Section 50.21: Procedures governing the destruction of contraband drug evidence in the custody of Federal law enforcement authorities.

(a) General.
The procedures set forth below are intended as a statement of policy of the Department of Justice and will be applied by the Department in exercising its responsibilities under Federal law relating to the destruction of seized contraband drugs.
(b) Purpose.
This policy implements the authority of the Attorney General under title I, section 1006(c)(3) of the Anti-Drug Abuse Act of 1986, Public Law 99-570 which is codified at 21 U.S.C. 881(f)(2), to direct the destruction, as necessary, of Schedule I and II contraband substances.

(c) Policy.
This regulation is intended to prevent the warehousing of large quantities of seized contraband drugs which are unnecessary for due process in criminal cases. Such stockpiling of contraband drugs presents inordinate security and storage problems which create additional economic burdens on limited law enforcement resources of the United States.

(d) Definitions.
As used in this subpart, the following terms shall have the meanings specified:

1. The term Contraband drugs are those controlled substances listed in Schedules I and II of the Controlled Substances Act seized for violation of that Act.

2. The term Marijuana is as defined in 21 U.S.C. 801(15) but does not include, for the purposes of this regulation, the derivatives hashish or hashish oil for purposes of destruction.

3. The term Representative sample means the exemplar for testing and a sample aggregate portion of the whole amount seized sufficient for current criminal evidentiary practice.

4. The term Threshold amount means:

   (i) Two kilograms of a mixture or substance containing a detectable amount of heroin;

   (ii) Ten kilograms of a mixture or substance containing a detectable amount of—

   (A) Coca leaves, except coca leaves and extracts of coca leaves from which cocaine, ecgonine, and derivatives of ecgonine or their salts have been removed;

   (B) Cocaine, its salts, optical and geometric isomers, and salts of isomers;

   (C) Ecgonine, its derivatives, their salts, isomers, and salts of isomers; or
(D) Any compound, mixture, or preparation which contains any quantity of any of the substances referred to in paragraphs (d)(4)(ii) (A) through (C) of this section;

(iii) Ten kilograms of a mixture or substance described in paragraph (d)(4)(ii)(B) of this section which contains cocaine base;

(iv) Two hundred grams of powdered phencyclidine (PCP) or two kilograms of a powdered mixture or substance containing a detectable amount of phencyclidine (PCP) or 28.35 grams of a liquid containing a detectable amount of phencyclidine (PCP);

(v) Twenty grams of a mixture or substance containing a detectable amount of Lysergic Acid Diethylamide (LSD);

(vi) Eight hundred grams of a mixture or substance containing a detectable amount of N-phenyl-N[1-(2-phenylethyl)-4-piperidinyl] propanamide (commonly known as fentanyl) or two hundred grams of a mixture or substance containing a detectable amount of any analogue of N-phenyl-N-[1-(2-phenylethyl)-4-piperidinyl propanamide; or

(vii) Twenty kilograms of hashish or two kilograms of hashish oil (21 U.S.C. 841(b)(1)(D), 960(b)(4)).

In the event of any changes to section 401(b)(1) of the Controlled Substances Act (21 U.S.C. 841(b)(1) as amended occurring after the date of these regulations, the threshold amount of any substance therein listed, except marijuana, shall be twice the minimum amount required for the most severe mandatory minimum sentence.

(e) Procedures.
Responsibilities of the Federal Bureau of Investigation and Drug Enforcement Administration.

When contraband drug substances in excess of the threshold amount or in the case of marijuana a quantity in excess of the representative sample are seized pursuant to a criminal investigation and retained in the custody of the Federal Bureau of Investigation or Drug Enforcement Administration, the Agency having custody shall:

(1) Immediately notify the appropriate U.S. Attorney, Assistant U.S. Attorney, or the responsible state/local prosecutor that the amount of seized contraband drug exceeding the threshold amount and its packaging, will be destroyed after sixty days from the date notice is provided of the seizures, unless
the agency providing notice is requested in writing by the authority receiving notice not to destroy the excess contraband drug; and

(2) Assure that appropriate tests of samples of the drug are conducted to determined the chemical nature of the contraband substance and its weight sufficient to serve as evidence before the trial courts of that jurisdiction; and

(3) Photographically depict, and if requested by the appropriate prosecutorial authority, videotape, the contraband drugs as originally packaged or an appropriate display of the seized contraband drugs so as to create evidentiary exhibits for use at trial; and

(4) Isolate and retain the appropriate threshold amounts of contraband drug evidence when an amount greater than the appropriate threshold amount has been seized, or when less than the appropriate threshold amounts of contraband drugs have been seized, the entire amount of the seizure, with the exception of marijuana, for which a representative sample shall be retained; and

(5) Maintain the retained portions of the contraband drugs until the evidence is no longer required for legal proceedings, at which time it may be destroyed, first having obtained consent of the U.S. Attorney, an Assistant U.S. Attorney, or the responsible state/local prosecutor;

(6) Notify the appropriate U.S. Attorney, Assistant U.S. Attorney, or the responsible state/local prosecutor to obtain consent to destroy the retained amount or representative sample whenever the related suspect(s) has been a fugitive from justice for a period of five years. An exemplar sufficient for testing will be retained consistent with this section.

(f) Procedures.
Responsibilities of the U.S. Attorney or the District Attorney (or equivalent state/local prosecutorial authority). When so notified by the Federal Bureau of Investigation or the Drug Enforcement Administration of an intent to destroy excess contraband drugs, the U.S. Attorney or the District Attorney (or equivalent) may:

(1) Agree to the destruction of the contraband drug evidence in excess of the threshold amount, or for marijuana in excess of the representative sample, prior to the normal sixty-day period. The U.S. Attorney, or the District Attorney (or equivalent) may delegate to his/her assistants authority to enter into such agreement; or

(2) Request an exception to the destruction policy in writing to the Special Agent in Charge of the responsible division prior to the end of the sixty-day period when retaining only the threshold amount or representative sample will significantly affect any legal proceedings; and
(3) In the event of a denial of the request may appeal the denial to the Assistant Attorney General, Criminal Division. Such authority may not be redelegated. An appeal shall stay the destruction until the appeal is complete.

(g) Supplementary regulations.
The Federal Bureau of Investigation and the Drug Enforcement Administration are authorized to issue regulations and establish procedures consistent with this section.

Official Citation:

28 CFR Section 50.22: Young American Medals Program.

(a) Scope.
There are hereby established two medals, one to be known as the Young American Medal for Bravery and the other to be known as the Young American Medal for Service.

(b) Young American Medal for Bravery.
(1)(i) The Young American Medal for Bravery may be awarded to a person—

(A) Who during a given calendar year has exhibited exceptional courage, attended by extraordinary decisiveness, presence of mind, and unusual swiftness of action, regardless of his or her own personal safety, in an effort to save or in saving the life of any person or persons in actual imminent danger;

(B) Who was eighteen years of age or younger at the time of the occurrence; and

(C) Who habitually resides in the United States (including its territories and possessions), but need not be a citizen thereof.

(ii) These conditions must be met at the time of the event.

(2) The act of bravery must have been public in nature and must have been acknowledged by the Governor, Chief Executive Officer of a State, county, municipality, or other political subdivision, or by a civic, educational, or religious institution, group, or society.
(3) No more than two such medals may be awarded in any one calendar year.

(c) Young American Medal for Service.
   (1) The Young American Medal for Service may be awarded to any citizen of the United States eighteen years of age or younger at the time of the occurrence, who has achieved outstanding or unusual recognition for character and service during a given calendar year.

   (2) Character attained and service accomplished by a candidate for this medal must have been such as to make his or her achievement worthy of public report. The outstanding and unusual recognition of the candidate's character and service must have been public in nature and must have been acknowledged by the Governor, Chief Executive Officer of a State, county, municipality, or other political subdivision, or by a civic, educational, or religious institution, group, or society.

   (3) The recognition of the character and service upon which the award of the Medal for Service is based must have been accorded separately and apart from the Young American Medals program and must not have been accorded for the specific and announced purpose of rendering a candidate eligible, or of adding to a candidate's qualifications, for the award of the Young American Medal for Service.

(4) No more than two such medals may be awarded in any one calendar year.

(d) Eligibility.
   (1) The act or acts of bravery and the recognition for character and service that make a candidate eligible for the respective medals must have occurred during the calendar year for which the award is made.

   (2) A candidate may be eligible for both medals in the same year. Moreover, the receipt of either medal in any year will not affect a candidate's eligibility for the award of either or both of the medals in a succeeding year.

   (3) Acts of bravery performed and recognition of character and service achieved by persons serving in the Armed Forces, which arise from or out of military duties, shall not make a candidate eligible for either of the medals, provided, however, that a person serving in the Armed Forces shall be eligible to receive either or both of the medals if the act of bravery performed or the recognition for character and service achieved is on account of acts and service performed or rendered outside of and apart from military duties.

(e) Request for information.
(1) A recommendation in favor of a candidate for the award of a Young American Medal for Bravery or for Service must be accompanied by:

(i) A full and complete statement of the candidate's act or acts of bravery or recognized character and service (including the times and places) that supports qualification of the candidate to receive the appropriate medal;

(ii) Statements by witnesses or persons having personal knowledge of the facts surrounding the candidate's act or acts of bravery or recognized character and service, as required by the respective medals;

(iii) A certified copy of the candidate's birth certificate, or, if no birth certificate is available, other authentic evidence of the date and place of the candidate's birth; and

(iv) A biographical sketch of the candidate, including information as to his or her citizenship or habitual residence, as may be required by the respective medals.

(f) Procedure.

(1)(i) All recommendations and accompanying documents and papers should be submitted to the Governor or Chief Executive Officer of the State, territory, or possession of the United States where the candidate's act or acts of bravery or recognized character and service were demonstrated. In the case of the District of Columbia, the recommendations should be submitted to the Mayor of the District of Columbia.

(ii) If the act or acts of bravery or recognized character and service did not occur within the boundaries of any State, territory, or possession of the United States, the papers should be submitted to the Governor or Chief Executive Officer of the territory or other possession of the United States wherein the candidate habitually maintains his or her residence.

(2) The Governor or Chief Executive Officer, after considering the various recommendations received after the close of the pertinent calendar year, may nominate therefrom no more than two candidates for the Young American Medal for Bravery and no more than two candidates for the Young American Medal for Service. Nominated individuals should have, in the opinion of the appropriate official, shown by the facts and circumstances to be the most worthy and qualified candidates from the jurisdiction to receive consideration for awards of the above-named medals.

(3) Nominations of candidates for either medal must be submitted no later than 120 days after notification that the Department of Justice is seeking nominations under this program for a specific calendar year. Each nomination
must contain the necessary documentation establishing eligibility, must be submitted by the Governor or Chief Executive Officer, together with any comments, and should be submitted to the address published in the notice.

(4) Nominations of candidates for medals will be considered only when received from the Governor or Chief Executive Officer of a State, territory, or possession of the United States.

(5) The Young American Medals Committee will select, from nominations properly submitted, those candidates who are shown by the facts and circumstances to be eligible for the award of the medals. The Committee shall make recommendations to the Attorney General based on its evaluation of the nominees. Upon consideration of these recommendations, the Attorney General may select up to the maximum allowable recipients for each medal for the calendar year.

(g) Presentation.
(1) The Young American Medal for Bravery and the Young American Medal for Service will be presented personally by the President of the United States to the candidates selected. These medals will be presented in the name of the President and the Congress of the United States. Presentation ceremonies shall be held at such times and places selected by the President in consultation with the Attorney General.

(2) The Young American Medals Committee will officially designate two adults (preferably the parents of the candidate) to accompany each candidate selected to the presentation ceremonies. The candidates and persons designated to accompany them will be furnished transportation and other appropriate allowances.

(3) There shall be presented to each recipient an appropriate Certificate of Commendation stating the circumstances under which the act of bravery was performed or describing the outstanding recognition for character and service, as appropriate for the medal awarded. The Certificate will bear the signature of the President of the United States and the Attorney General of the United States.

(4) There also shall be presented to each recipient of a medal, a miniature replica of the medal awarded in the form of a lapel pin.

(h) Posthumous awards.
In cases where a medal is awarded posthumously, the Young American Medals Committee will designate the father or mother of the deceased or other suitable person to receive the medal on behalf of the deceased. The decision of the Young American Medals Committee in designating the person to receive the posthumously awarded medal, on behalf of the deceased, shall be final.
(i) Young American Medals Committee.
The Young American Medals Committee shall be represented by the following:

(1) Director of the FBI, Chairman;

(2) Administrator of the Drug Enforcement Administration, Member;

(3) Director of the U.S. Marshals Service, Member; and

(4) Assistant Attorney General, Office of Justice Programs, Member and Executive Secretary.

Authority:
Authority: The United States Department of Justice is authorized under 42 U.S.C. 1921 et seq. to promulgate rules and regulations establishing medals, one for bravery and one for service. This authority was enacted by chapter 520 of Pub. L. 81-638 (August 3, 1950).

Official Citation:
[61 FR 49260, Sept. 19, 1996]

28 CFR Section 50.23: Policy against entering into final settlement agreements or consent decrees that are subject to confidentiality provisions and against seeking or concurring in the sealing of such documents.

(a) It is the policy of the Department of Justice that, in any civil matter in which the Department is representing the interests of the United States or its agencies, it will not enter into final settlement agreements or consent decrees that are subject to confidentiality provisions, nor will it seek or concur in the sealing of such documents. This policy flows from the principle of openness in government and is consistent with the Department's policies regarding openness in judicial proceedings (see 28 CFR 50.9) and the Freedom of Information Act (see Memorandum for Heads of Departments and Agencies from the Attorney General Re: The Freedom of Information Act (Oct. 4, 1993)).

(b) There may be rare circumstances that warrant an exception to this general rule. In determining whether an exception is appropriate, any such circumstances must be considered in the context of the public's strong interest in knowing about the conduct of its Government and expenditure of its resources. The existence of such circumstances must be documented as part of the approval process, and any confidentiality provision must be drawn as narrowly as possible. Non-delegable approval authority to determine that an exception justifies use of a confidentiality
provision in, or seeking or concurring in the sealing of, a final settlement or consent decree resides with the relevant Assistant Attorney General or United States Attorney, unless authority to approve the settlement itself lies with a more senior Department official, in which case the more senior official will have such approval authority.

(c) Regardless of whether particular information is subject to a confidentiality provision or to seal, statutes and regulations may prohibit its disclosure from Department of Justice files. Thus, before releasing any information, Department attorneys should consult all appropriate statutes and regulations (e.g., 5 U.S.C. 552a (Privacy Act); 50 U.S.C. 403-3(c)(6) (concerning intelligence sources and methods), and Execution Order 12958 (concerning national security information). In particular, in matters involving individuals, the Privacy Act regulates disclosure of settlement agreements that have not been made part of the court record.

(d) The principles set forth in this section are intended to provide guidance to attorneys for the Government and are not intended to create or recognize any legally enforceable right in any person.

**Official Citation:**
[Order No. 2270-99, 64 FR 59122, Nov. 2, 1999]

**28 CFR Section 50.24: Annuity broker minimum qualifications.**

(a) Minimum standards.
The Civil Division, United States Department of Justice, shall establish a list of annuity brokers who meet minimum qualifications for providing annuity brokerage services in connection with structured settlements entered by the United States. Those qualifications are as follows:

(1) The broker must have a current license issued by at least one State, the District of Columbia, or a Territory of the United States as a life insurance agent, producer, or broker;

(2) The broker must have a current license or appointment issued by at least one life insurance company to sell its structured settlement annuity contracts or to act as a structured settlement consultant or broker for the company;

(3) The broker must be currently covered by an Errors and Omissions insurance policy, or an equivalent form of insurance;
(4) The broker must never have had a license to be a life insurance agent, producer, or broker revoked, rescinded, or suspended for any reason or for any period of time;

(5) The broker must not have been convicted of a felony; and

(6) The broker must have had substantial experience in each of the past three years in providing structured settlement brokerage services to or on behalf of defendants or their counsel.

(b) Procedures for inclusion on the list.
(1) An annuity broker who desires to be included on the list must submit a “Declaration” that he or she has reviewed the list of minimum qualifications set forth in paragraph (a) of this section and that he or she meets those minimum qualifications. A sample of the Declaration for annuity brokers to submit is available from the Civil Division’s Web site (http://www.usdoj.gov/civil/home.html) or by written request to the address in this section. These minimum qualifications must be continually met for a broker who has been included on the list to remain included when the list is updated thereafter. The Declaration must be executed under penalty of perjury in a manner specified in 28 U.S.C. 1746.

(2) Each broker must submit a new Declaration annually to be included on updated lists. For a broker to be included on the initial list to be established by May 1, 2003, the Torts Branch, Civil Division, must receive the broker's Declaration no later than April 24, 2003. If the broker wishes to be included on updated lists, the Torts Branch must receive a new Declaration from the broker between January 1 and April 10 of each successive calendar year. After the Declaration is completed and signed, the original must be mailed to the United States Department of Justice, Civil Division, FTCA Staff, Post Office Box 888, Benjamin Franklin Station, Washington, DC 20044. The Department of Justice will not accept a photocopy or facsimile of the Declaration.

(3) A Declaration will not be accepted by the Department of Justice unless it is complete and has been signed by the individual annuity broker requesting inclusion on the list. A Declaration that is incomplete or has been altered, amended, or changed in any respect from the Declaration at the Civil Division's Web site will not be accepted by the Department of Justice. Such a Declaration will be returned to the annuity broker who submitted it, and the Department of Justice will take no further action on the request for inclusion on the list until the defect in the Declaration has been cured by the annuity broker.

(4) The Department of Justice will retain a complete Declaration signed and filed by an annuity broker requesting to be on the list. Because this rule does not require the submission of any additional information, the Department retains
discretion to dispose of additional information or documentation provided by an annuity broker.

(5) The Department of Justice will not accept a Declaration submitted by an annuity company or by someone on behalf of another individual or group of individuals. Each individual annuity broker who desires to be included on the list must submit his or her own Declaration.

(6) An annuity broker whose name appears on the list incorrectly may submit a written request that his or her name be corrected. An annuity broker whose name appears on the list may submit a written request that his or her name be removed from the list.

(7) To the extent practicable, a name correction or deletion will appear on the next revision of the list immediately after receipt of the written request for a name correction or deletion. A written request for a name correction or deletion must be mailed to the United States Department of Justice, Civil Division, FTCA Staff, Post Office Box 888, Benjamin Franklin Station, Washington, DC 20044. Facsimiles will not be accepted.

(8) The list of annuity brokers established pursuant to this section will be updated periodically, but not more often than twice every calendar year, beginning in calendar year 2004.

(c) Disclaimers.

(1) The inclusion of an annuity broker on the list signifies only that the individual declared under penalty of perjury that he or she meets the minimum qualifications required by the Attorney General for providing annuity brokerage services in connection with structured settlements entered into by the United States. Because the decision to include an individual annuity broker on the list is based solely and exclusively on the Declaration submitted by the annuity broker, the appearance of an annuity broker's name on the list does not signify that the annuity broker actually meets those minimum qualifications or is otherwise competent to provide structured settlement brokerage services to the United States. No preferential consideration will be given to an annuity broker appearing on the list except to the extent that United States Attorneys utilize the list pursuant to section 11015(b) of Public Law 107-273.

(2) By submitting a Declaration to the Department of Justice, the individual annuity broker agrees that the Declaration and the list each may be made public in its entirety, and the annuity broker expressly consents to such release and disclosure of the Declaration and list.

Official Citation:
[Order No. 2667-2003, 68 FR 18120, Apr. 15, 2003]
28 CFR Section 52.01: Civil proceedings: Special master, pretrial, trial, appeal.

(a) Sections 636 (b) and (c) of title 28 of the United States Code govern pretrial and case-dispositive civil jurisdiction of magistrate judges, as well as service by magistrate judges as special masters.

(b) It is the policy of the Department of Justice to encourage the use of magistrate judges, as set forth in this paragraph, to assist the district courts in resolving civil disputes. In conformity with this policy, the attorney for the government is encouraged to accede to a referral of an entire civil action for disposition by a magistrate judge, or to consent to designation of a magistrate judge as special master, if the attorney, with the concurrence of his or her supervisor, determines that such a referral or designation is in the interest of the United States. In making this determination, the attorney shall consider all relevant factors, including—

(1) The complexity of the matter, including involvement of significant rights of large numbers of persons;

(2) The relief sought;

(3) The amount in controversy;

(4) The novelty, importance, and nature of the issues raised;

(5) The likelihood that referral to or designation of the magistrate judge will expedite resolution of the litigation;

(6) The experience and qualifications of the magistrate judge; and

(7) The possibility of the magistrate judge’s actual or apparent bias or conflict of interest.
(c)(1) In determining whether to consent to having an appeal taken to the district court rather than to the court of appeals, the attorney for the government should consider all relevant factors including—

(i) The amount in controversy;

(ii) The importance of the questions of law involved;

(iii) The desirability of expeditious review of the magistrate judge's judgment.

(2) In making a determination under paragraph (c)(1) of this section the attorney shall, except in those cases in which delegation authority has been exercised under 28 CFR 0.168, consult with the Assistant Attorney General having supervisory authority over the subject matter.

Official Citation:
(i) The novelty of the case with respect to the facts, the statute being enforced, and the application of the statute to the facts;

(ii) The importance of the case in light of the nature and seriousness of the offense charged;

(iii) The defendant’s history of criminal activity, the potential penalty upon conviction, and the purposes to be served by prosecution, including punishment, deterrence, rehabilitation, and incapacitation;

(iv) The factual and legal complexity of the case and the amount and nature of the evidence to be presented;

(v) The desirability of prompt disposition of the case; and

(vi) The experience and qualifications of the magistrate judge, and the possibility of the magistrate judge’s actual or apparent bias or conflict of interest.

(2) The attorney for the government shall consult with the Assistant Attorney General having supervisory authority over the subject matter in determining whether to petition for trial before a district judge in a case involving a violation of 2 U.S.C. 192, 441j(a); 18 U.S.C. 210, 211, 242, 245, 594, 597, 599, 600, 601, 1304, 1504, 1508, 1509, 2234, 2235, 2236; or 42 U.S.C. 3631.

(3) In a case in which the government petitions for trial before a district judge, the attorney for the government shall forward a copy of the petition to the Assistant Attorney General having supervisory authority over the subject matter and, if the petition is denied, shall promptly notify the Assistant Attorney General.

Authority: (5 U.S.C. 301, 18 U.S.C. 3401(f))

Official Citation:
28 CFR PART 59—GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES

- 28 CFR Section 59.1: Introduction.
- 28 CFR Section 59.2: Definitions.
- 28 CFR Section 59.3: Applicability.
- 28 CFR Section 59.4: Procedures.
- 28 CFR Section 59.5: Functions and authorities of the Deputy Assistant Attorneys General.
- 28 CFR Section 59.6: Sanctions.

Authority:

Source:
Order No. 942-81, 46 FR 22364, Apr. 17, 1981, unless otherwise noted.

28 CFR Section 59.1: Introduction.

(a) A search for documentary materials necessarily involves intrusions into personal privacy. First, the privacy of a person's home or office may be breached. Second, the execution of such a search may require examination of private papers within the scope of the search warrant, but not themselves subject to seizure. In addition, where such a search involves intrusions into professional, confidential relationships, the privacy interests of other persons are also implicated.

(b) It is the responsibility of federal officers and employees to recognize the importance of these personal privacy interests, and to protect against unnecessary intrusions. Generally, when documentary materials are held by a disinterested third party, a subpoena, administrative summons, or governmental request will be an effective alternative to the use of a search warrant and will be considerably less intrusive. The purpose of the guidelines set forth in this part is to assure that federal officers and employees do not use search and seizure to obtain documentary materials in the possession of disinterested third parties unless reliance on alternative means would substantially jeopardize their availability (e.g., by creating a risk of destruction, etc.) or usefulness (e.g., by detrimentally delaying the investigation, destroying a chain of custody, etc.). Therefore, the guidelines in this part establish certain criteria and procedural requirements which must be met before a search warrant may be used to obtain documentary materials held by disinterested third parties. The guidelines in this
part are not intended to inhibit the use of less intrusive means of obtaining documentary materials such as the use of a subpoena, summons, or formal or informal request.

28 CFR Section 59.2: Definitions.

As used in this part—

(a) The term attorney for the government shall have the same meaning as is given that term in Rule 54(c) of the Federal Rules of Criminal Procedure;

(b) The term disinterested third party means a person or organization not reasonably believed to be—

(1) A suspect in the criminal offense to which the materials sought under these guidelines relate; or

(2) Related by blood or marriage to such a suspect;

(c) The term documentary materials means any materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, films or negatives, audio or video tapes, or materials upon which information is electronically or magnetically recorded, but does not include materials which constitute contraband, the fruits or instrumentalities of a crime, or things otherwise criminally possessed;

(d) The term law enforcement officer shall have the same meaning as the term “federal law enforcement officer” as defined in Rule 41(h) of the Federal Rules of Criminal Procedure; and

(e) The term supervisory official of the Department of Justice means the supervising attorney for the section, office, or branch within the Department of Justice which is responsible for the investigation or prosecution of the offense at issue, or any of his superiors.

28 CFR Section 59.3: Applicability.

(a) The guidelines set forth in this part apply, pursuant to section 201 of the Privacy Protection Act of 1980 (Sec. 201, Pub. L. 96-440, 94 Stat. 1879, (42 U.S.C. 2000aa-11)), to the procedures used by any federal officer or employee, in connection with the investigation or prosecution of a criminal offense, to obtain documentary materials in the private possession of a disinterested third party.
(b) The guidelines set forth in this part do not apply to:

(1) Audits, examinations, or regulatory, compliance, or administrative inspections or searches pursuant to federal statute or the terms of a federal contract;

(2) The conduct of foreign intelligence or counterintelligence activities by a government authority pursuant to otherwise applicable law;

(3) The conduct, pursuant to otherwise applicable law, of searches and seizures at the borders of, or at international points of entry into, the United States in order to enforce the customs laws of the United States;

(4) Governmental access to documentary materials for which valid consent has been obtained; or

(5) Methods of obtaining documentary materials whose location is known but which have been abandoned or which cannot be obtained through subpoena or request because they are in the possession of a person whose identity is unknown and cannot with reasonable effort be ascertained.

(c) The use of search and seizure to obtain documentary materials which are believed to be possessed for the purpose of disseminating to the public a book, newspaper, broadcast, or other form of public communication is subject to title I of the Privacy Protection Act of 1980 (Sec. 101, et seq., Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa, et seq.)), which strictly prohibits the use of search and seizure to obtain such materials except under specified circumstances.

(d) These guidelines are not intended to supersede any other statutory, regulatory, or policy limitations on access to, or the use or disclosure of particular types of documentary materials, including, but not limited to, the provisions of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401, et seq.), the Drug Abuse Office and Treatment Act of 1972, as amended (21 U.S.C. 1101, et seq.), and
the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970, as amended (42 U.S.C. 4541, et seq.).

28 CFR Section 59.4: Procedures.8

(a) Provisions governing the use of search warrants generally.

(1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party unless it appears that the use of a subpoena, summons, request, or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought, and the application for the warrant has been authorized as provided in paragraph (a)(2) of this section.

(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party unless the application for the warrant has been authorized by an attorney for the government. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of an attorney for the government, the application may be authorized by a supervisory law enforcement officer in the applicant’s department or agency, if the appropriate U.S. Attorney (or where the case is not being handled by a U.S. Attorney’s Office, the appropriate supervisory official of the Department of Justice) is notified of the authorization and the basis for justifying such authorization under this part within 24 hours of the authorization.

(b) Provisions governing the use of search warrants which may intrude upon professional, confidential relationships.

---

8 Notwithstanding the provisions of this section, any application for a warrant to search for evidence of a criminal tax offense under the jurisdiction of the Tax Division must be specifically approved in advance by the Tax Division pursuant to section 6-2.330 of the U.S. Attorneys’ Manual.
(1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman, under circumstances in which the materials sought, or other materials likely to be reviewed during the execution of the warrant, contain confidential information on patients, clients, or parishioners which was furnished or developed for the purposes of professional counseling or treatment, unless—

(i) It appears that the use of a subpoena, summons, request or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought;

(ii) Access to the documentary materials appears to be of substantial importance to the investigation or prosecution for which they are sought; and

(iii) The application for the warrant has been approved as provided in paragraph (b)(2) of this section.

(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman under the circumstances described in paragraph (b)(1) of this section, unless, upon the recommendation of the U.S. Attorney (or where a case is not being handled by a U.S. Attorney's Office, upon the recommendation of the appropriate supervisory official of the Department of Justice), an appropriate Deputy Assistant Attorney General has authorized the application for the warrant. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of a Deputy Assistant Attorney General, the application may be authorized by the U.S. Attorney (or where the case is not being handled by a U.S. Attorney's Office, by the appropriate supervisory official of the Department of Justice) if an appropriate Deputy Assistant Attorney General is notified of the authorization

---

Documentary materials created or compiled by a physician, but retained by the physician as a matter of practice at a hospital or clinic shall be deemed to be in the private possession of the physician, unless the clinic or hospital is a suspect in the offense.
and the basis for justifying such authorization under this part within 72 hours of the authorization.

(3) Whenever possible, a request for authorization by an appropriate Deputy Assistant Attorney General of a search warrant application pursuant to paragraph (b)(2) of this section shall be made in writing and shall include:

(i) The application for the warrant; and

(ii) A brief description of the facts and circumstances advanced as the basis for recommending authorization of the application under this part.

If a request for authorization of the application is made orally or if, in an emergency situation, the application is authorized by the U.S. Attorney or a supervisory official of the Department of Justice as provided in paragraph (b)(2) of this section, a written record of the request including the materials specified in paragraphs (b)(3)(i) and (ii) of this section shall be transmitted to an appropriate Deputy Assistant Attorney General within 7 days. The Deputy Assistant Attorneys General shall keep a record of the disposition of all requests for authorizations of search warrant applications made under paragraph (b) of this section.

(4) A search warrant authorized under paragraph (b)(2) of this section shall be executed in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials.

(5) Although it is impossible to define the full range of additional doctor-like therapeutic relationships which involve the furnishing or development of private information, the U.S. Attorney (or where a case is not being handled by a U.S. Attorney's Office, the appropriate supervisory official of the Department of Justice) should determine whether a search for documentary materials held by other disinterested third party professionals involved in such relationships (e.g. psychologists or psychiatric social workers or nurses) would implicate the special privacy concerns which are addressed in paragraph (b) of this section. If the U.S. Attorney (or other supervisory official of the Department of Justice) determines that such a search would require review of extremely confidential information furnished or developed for the purposes of professional counseling or treatment, the provisions of this subsection should be applied. Otherwise, at a minimum, the requirements of paragraph (a) of this section must be met.

(c) Considerations bearing on choice of methods. In determining whether, as an alternative to the use of a search warrant, the use of a subpoena or other less intrusive means of obtaining documentary materials would substantially jeopardize the availability or usefulness of the materials sought, the following factors, among others, should be considered:
(1) Whether it appears that the use of a subpoena or other alternative which gives advance notice of the government's interest in obtaining the materials would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought; considerations, among others, bearing on this issue may include:

(i) Whether a suspect has access to the materials sought;

(ii) Whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect;

(iii) Whether the possessor of the materials is under the domination or control of a suspect;

(iv) Whether the possessor of the materials has an interest in preventing the disclosure of the materials to the government;

(v) Whether the possessor's willingness to comply with a subpoena or request by the government would be likely to subject him to intimidation or threats of reprisal;

(vi) Whether the possessor of the materials has previously acted to obstruct a criminal investigation or judicial proceeding or refused to comply with or acted in defiance of court orders; or

(vii) Whether the possessor has expressed an intent to destroy, conceal, alter, or transfer the materials;

(2) The immediacy of the government's need to obtain the materials; considerations, among others, bearing on this issue may include:

(i) Whether the immediate seizure of the materials is necessary to prevent injury to persons or property;

(ii) Whether the prompt seizure of the materials is necessary to preserve their evidentiary value;

(iii) Whether delay in obtaining the materials would significantly jeopardize an ongoing investigation or prosecution; or

(iv) Whether a legally enforceable form of process, other than a search warrant, is reasonably available as a means of obtaining the materials.

The fact that the disinterested third party possessing the materials may have grounds to challenge a subpoena or other legal process is not in itself a legitimate basis for the use of a search warrant.
28 CFR Section 59.5: Functions and authorities of the Deputy Assistant Attorneys General.

The functions and authorities of the Deputy Assistant Attorneys General set out in this part may at any time be exercised by an Assistant Attorney General, the Associate Attorney General, the Deputy Attorney General, or the Attorney General.

28 CFR Section 59.6: Sanctions.

(a) Any federal officer or employee violating the guidelines set forth in this part shall be subject to appropriate disciplinary action by the agency or department by which he is employed.

(b) Pursuant to section 202 of the Privacy Protection Act of 1980 (sec. 202, Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa-12)), an issue relating to the compliance, or the failure to comply, with the guidelines set forth in this part may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion of evidence.
28 CFR PART 60—AUTHORIZATION OF FEDERAL LAW ENFORCEMENT OFFICERS TO REQUEST THE ISSUANCE OF A SEARCH WARRANT

- 28 CFR Section 60.1: Purpose.
- 28 CFR Section 60.2: Authorized categories.
- 28 CFR Section 60.3: Agencies with authorized personnel.

Authority:

28 CFR Section 60.1: Purpose.

This regulation authorizes certain categories of federal law enforcement officers to request the issuance of search warrants under Rule 41, Fed. R. Crim. P., and lists the agencies whose officers are so authorized. Rule 41(a) provides in part that a search warrant may be issued “upon the request of a federal law enforcement officer,” and defines that term in Rule 41(h) as “any government agent, *** who is engaged in the enforcement of the criminal laws and is within the category of officers authorized by the Attorney General to request the issuance of a search warrant.” The publication of the categories and the listing of the agencies is intended to inform the courts of the personnel who are so authorized. It should be noted that only in the very rare and emergent case is the law enforcement officer permitted to seek a search warrant without the concurrence of the appropriate U.S. Attorney’s office. Further, in all instances, military agents of the Department of Defense must obtain the concurrence of the appropriate U.S. Attorney’s Office before seeking a search warrant.

Official Citation:
[Order No. 826-79, 44 FR 21785, Apr. 12, 1979, as amended by Order No. 1026-83, 48 FR 37377, Aug. 18, 1983]

28 CFR Section 60.2: Authorized categories.

The following categories of federal law enforcement officers are authorized to request the issuance of a search warrant:

(a) Any person authorized to execute search warrants by a statute of the United States.
(b) Any person who has been authorized to execute search warrants by the head of a department, bureau, or agency (or his delegate, if applicable) pursuant to any statute of the United States.

(c) Any peace officer or customs officer of the Virgin Islands, Guam, or the Canal Zone.

(d) Any officer of the Metropolitan Police Department, District of Columbia.

(e) Any person authorized to execute search warrants by the President of the United States.

(f) Any civilian agent of the Department of Defense not subject to military direction who is authorized by statute or other appropriate authority to enforce the criminal laws of the United States.

(g) Any civilian agent of the Department of Defense who is authorized to enforce the Uniform Code of Military Justice.

(h) Any military agent of the Department of Defense who is authorized to enforce the Uniform Code of Military Justice.

(i) Any special agent of the Office of Inspector General, Department of Transportation.

(j) Any special agent of the Investigations Division of the Office of Inspector General, Small Business Administration.


(m) Any special agent of the Office of Inspector General, Department of Housing and Urban Development.

(n) Any special agent of the Office of Inspector General, Department of Interior.

(o) Any special agent of the Office of Inspector General, Veterans Administration.

(p) Any special agent of the Office of Inspector General, Social Security Administration.
(q) Any special agent of the Office of Inspector General, Department of Health and Human Services.

**Official Citation:**

**28 CFR Section 60.3: Agencies with authorized personnel.**

The following agencies have law enforcement officers within the categories listed in § 60.2 of this part:

(a) National Law Enforcement Agencies:
(1) Department of Agriculture:
   National Forest Service
   Office of the Inspector General
(2) Department of Defense:
   Defense Investigative Service Criminal Investigation Command, U.S. Army
   Naval Investigative Service, U.S. Navy
   Office of Special Investigation, U.S. Air Force
(3) Department of Health and Human Services:
   Center for Disease Control
   Food and Drug Administration
   Office of Investigations, Office of the Inspector General
(4) Department of the Interior:
   Bureau of Indian Affairs
   Bureau of Sport Fisheries and Wildlife
   National Park Service
(5) Department of Justice:
   Drug Enforcement Administration
   Federal Bureau of Investigation
   Immigration and Naturalization Service
   U.S. Marshals Service
(6) Department of Transportation:
   U.S. Coast Guard
   Office of Inspector General, Department of Transportation
(7) Department of the Treasury:
   Bureau of Alcohol, Tobacco, and Firearms
   Executive Protective Service
Internal Revenue Service
Criminal Investigation Division
Internal Security Division, Inspection Service
U.S. Customs Service
U.S. Secret Service

(8) U.S. Postal Service:
Inspection Service
Office of Inspector General

(9) Department of Commerce:
Office of Export Enforcement

(10) Small Business Administration:
Investigations Division of the Office of Inspector General

(11) Department of State:
Diplomatic Security Service

(12) Department of Labor:
Office of Investigations and Office of Labor Racketeering of the
Office of Inspector General

(13) General Services Administration:
Office of Inspector General

(14) Department of Housing and Urban Development:
Office of Inspector General

(15) Department of the Interior:
Office of Inspector General

(16) Veterans Administration:
Office of Inspector General

(17) Environmental Protection Agency:
Office of Criminal Investigations

(18) Social Security Administration,
Office of Inspector General

(b) Local Law Enforcement Agencies:

(1) District of Columbia Metropolitan Police Department

(2) Law Enforcement Forces and Customs Agencies of Guam, The Virgin
Islands, and the Canal Zone.

Official Citation:
[Order No. 826-79, 44 FR 21785, Apr. 12, 1979]

Editorial Note:
For Federal Register citations affecting § 60.3, see the List of CFR Sections
Affected, which appears in the Finding Aids section of the printed volume and at
www.fdsys.gov.
Subpart A—Eligible Applicants
  o 28 CFR Section 65.1: General.
  o 28 CFR Section 65.2: State Government.

Subpart B—Allocation of Funds and Other Assistance
  o 28 CFR Section 65.10: Fund availability.
  o 28 CFR Section 65.11: Limitations on fund and other assistance use.
  o 28 CFR Section 65.12: Other assistance.

Subpart C—Purpose of Emergency Federal Law Enforcement Assistance
  o 28 CFR Section 65.20: General.
  o 28 CFR Section 65.21: Purpose of assistance.
  o 28 CFR Section 65.22: Exclusions.

Subpart D—Application for Assistance
  o 28 CFR Section 65.30: General.
  o 28 CFR Section 65.31: Application content.

Subpart E—Submission and Review of Applications
  o 28 CFR Section 65.40: General.
  o 28 CFR Section 65.41: Review of State applications.

Subpart F—Additional Requirements
  o 28 CFR Section 65.50: General.
  o 28 CFR Section 65.51: Recordkeeping.
  o 28 CFR Section 65.52: Civil rights.
  o 28 CFR Section 65.53: Confidentiality of information.

Subpart G—Repayment of Funds
  o 28 CFR Section 65.60: Repayment of funds.

Subpart H—Definitions
  o 28 CFR Section 65.70: Definitions.

Subpart I—Immigration Emergency Fund
  o 28 CFR Section 65.80: General.
  o 28 CFR Section 65.81: General definitions.
  o 28 CFR Section 65.82: Procedure for requesting a Presidential determination of an immigration emergency.
  o 28 CFR Section 65.83: Assistance required by the Attorney General.
  o 28 CFR Section 65.84: Procedures for the Attorney General when seeking State or local assistance.
  o 28 CFR Section 65.85: Procedures for State or local governments applying for funding.

Authority:

Source:
50 FR 51340, Dec. 16, 1985, unless otherwise noted.
SUBPART A—Eligible Applicants

28 CFR Section 65.1: General.

This subject describes who may apply for emergency Federal law enforcement assistance under the Justice Assistance Act of 1984.

28 CFR Section 65.2: State Government.

In the event that a law enforcement emergency exists throughout a state or part of a state, a state (on behalf of itself or a local unit of government) may submit an application to the Attorney General, for emergency Federal law enforcement assistance. This application is to be submitted by the chief executive officer of the state, in writing, on Standard Form 424, and in accordance with these regulations.

SUBPART B—Allocation of Funds and Other Assistance

28 CFR Section 65.10: Fund availability.

For the previous fiscal year (FY '85), $800,000 was appropriated for emergency Federal law enforcement assistance for the entire country. In FY '86, $1.5 million has been requested. The FY '86 request has not yet been appropriated and is not currently available. The form and extent of assistance provided will be determined by the nature and scope of the emergency presented; but, in any event, no fund award may exceed the amount ultimately appropriated.

28 CFR Section 65.11: Limitations on fund and other assistance use.

(a) Land acquisition.
No funds shall be used for the purpose of land acquisition.

(b) Non-supplantation.
No funds shall be used to supplant state or local funds that would otherwise be made available for such purposes.

(c) Civil justice.
No funds or other assistance shall be used with respect to civil justice matters except to the extent that such civil justice matters bear directly and substantially
upon criminal justice matters or are inextricably intertwined with criminal justice matters.

    (d) Federal law enforcement personnel. Nothing in the enabling legislation authorizes the use of Federal law enforcement personnel to investigate violations of criminal law other than violations with respect to which investigation is authorized by other provisions of law. (section 609O(a), of the Act).

    (e) Direction, supervision, control. Nothing in the enabling legislation shall be construed to authorize the Attorney General or the Federal law enforcement community to exercise any direction, supervision, or control over any police force or other criminal justice agency of an applicant for Federal law enforcement assistance. (section 609O(b), of the Act).

28 CFR Section 65.12: Other assistance.

In accordance with the purposes and limitations of this subdivision, members of the Federal law enforcement community may provide needed assistance in the form of equipment, training, intelligence information, and personnel. The application may include requests for assistance of this nature.
SUBPART C—Purpose of Emergency Federal Law Enforcement Assistance

28 CFR Section 65.20: General.

The purpose of the Act is to assist state and/or local units of government which are experiencing law enforcement emergencies to respond to those emergencies through the provision of Federal law enforcement assistance. The authority and responsibility for implementation of this section is vested in the Attorney General of the United States.

28 CFR Section 65.21: Purpose of assistance.

The purpose of emergency Federal law enforcement assistance is to provide necessary assistance to (and through) a state government to provide an adequate response to an uncommon situation which requires law enforcement, which is or threatens to become of serious or epidemic proportions, and with respect to which state and local resources are inadequate to protect the lives and property of citizens, or to enforce the criminal law.

28 CFR Section 65.22: Exclusions.

Excluded from the situations for which this assistance is intended are:

(a) The perceived need for planning or other activities related to crowd control for general public safety projects; and,

(b) A situation requiring the enforcement of laws associated with scheduled public events, including political conventions and sports events.
SUBPART D—Application for Assistance
28 CFR Section 65.30: General.

The Act requires that applications be submitted in writing, by the chief executive officer of a state, on Standard Form 424, in accordance with these regulations.

28 CFR Section 65.31: Application content.

The Act identifies six factors which the Attorney General will consider in approving or disapproving an application, and includes administrative requirements to ensure appropriate use of Federal assistance. Therefore, each application must be in writing and must include the following:

(a) Problem.
A description of the nature and extent of the law enforcement emergency, including the specific identification and description of the political and geographical subdivision(s) wherein the emergency exists;

(b) Cause.
A description of the situation or extraordinary circumstances which produced such emergency;

(c) Resources.
A description of the state and local criminal justice resources available to address the emergency, and a discussion of why and to what degree they are insufficient;

(d) Assistance requested.
A specific statement of the funds, equipment, training, intelligence information, or personnel requested, and a description of their intended use;

(e) Other assistance.
The identification of any other assistance the state or appropriate unit of government has received, or could receive, under any provision of the Act; and,

(f) Other requirements.
Assurance of compliance with other requirements of the Act, detailed in other parts of these regulations, including: Nonsupplantation; nondiscrimination; confidentiality of information; prohibition against land acquisition; recordkeeping and audit; limitation on civil justice matters.
This subpart describes the process and criteria for the Attorney General’s review and approval or disapproval of state applications. The original application, on Standard Form 424, signed by the chief executive officer of the state should be submitted directly to the Attorney General, U.S. Department of Justice, Washington, DC 20503. One copy of the application should be sent to the Director, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, Washington, DC 20531.

Official Citation:
[67 FR 7270, Feb. 19, 2002]

28 CFR Section 65.41: Review of State applications.

(a) Review criteria.
The Act provides the basis for review and approval or disapproval of state applications. Federal law enforcement assistance may be provided if such assistance is necessary to provide an adequate response to a law enforcement emergency. In determining whether to approve or disapprove an application for assistance under this section, the Attorney General shall consider:

(1) The nature and extent of such emergency throughout a state or in any part of a state;

(2) The situation or extraordinary circumstances which produced such emergency;

(3) The availability of state and local criminal justice resources to resolve the problem;

(4) The cost associated with the increased Federal presence;

(5) The need to avoid unnecessary Federal involvement and intervention in matters primarily of state and local concern; and,

(6) Any assistance which the state or other appropriate unit of government has received, or could receive, under any provision of title I of the Omnibus Crime Control and Safe Streets Act of 1968.

(b) Review process.
(1) The Attorney General shall consult with the Assistant Attorney General, Office of Justice Programs, and the Director, Bureau of Justice Assistance, on requests for grant assistance.

(2) All requests for assistance of the Federal law enforcement community (e.g., equipment, training, information, or personnel) shall be reviewed by the Attorney General in consultation with appropriate members of the Federal law enforcement community, including the United States Attorney(s) in the affected District(s). Such requests will be subject to statutory restrictions, including section 609O on Federal agency activities.

(3) The Attorney General will approve or disapprove each application, submitted in accordance with these regulations, no later than ten (10) days after receipt.
This subpart sets forth additional requirements under the Justice Assistance Act. Applicants for assistance must assure compliance with each of these requirements.

28 CFR Section 65.51: Recordkeeping.

(a) The state must assure that it adheres to the recordkeeping requirements enumerated in OMB Circulars, Number A-102 and Number A-128. This requirement extends to participating units of local government, in that they are viewed as the state’s subgrantees.

(b) The Attorney General and the Comptroller of the United States shall have access, for the purpose of audit and examination, to any books, documents, and records of recipients of Federal law enforcement assistance provided under this subdivision which, in the opinion of the Attorney General or the Comptroller General, are related to the receipt or use of such assistance.

28 CFR Section 65.52: Civil rights.

The Act provides that “no person in any state shall on the grounds of race, color, religion, national origin, or sex be excluded from participation in, be denied the benefits of, or be subjected to discrimination under or denied employment in connection with any programs or activity funded in whole or in part with funds made available under this title.” Recipients of funds under the Act are also subject to the provisions of title VI of the Civil Rights Act of 1964; section 504 of the Rehabilitation Act of 1973, as amended; title IX of the Education Amendments of 1972; the Age Discrimination Act of 1975; and the Department of Justice Non-Discrimination Regulations 28 CFR part 42, subparts C, D, E, and G.

28 CFR Section 65.53: Confidentiality of information.

Section 812 of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended and implemented by 28 CFR part 20) shall apply with respect to information, including criminal history information and criminal intelligence systems operating with the support of Federal law enforcement assistance.
SUBPART G—Repayment of Funds
28 CFR Section 65.60: Repayment of funds.

(a) If Federal law enforcement assistance provided under this subdivision is used by the recipient of such assistance in violation of these regulations, or for any purpose other than the purpose for which it is provided, then such recipient shall promptly repay to the Attorney General an amount equal to the value of such assistance.

(b) The Attorney General may bring a civil action in an appropriate United States District Court to recover any amount authorized to be repaid under law.
(a) Law enforcement emergency.
The term law enforcement emergency is defined by the Act as an uncommon situation which requires law enforcement, which is or threatens to become of serious or epidemic proportions, and with respect to which state and local resources are inadequate to protect the lives and property of citizens, or to enforce the criminal law. The Act specifically excludes the following situations when defining “law enforcement emergency”:

(1) The perceived need for planning or other activities related to crowd control for general public safety projects; and,

(2) A situation requiring the enforcement of laws associated with scheduled public events, including political convention and sports events.

(b) Federal law enforcement assistance.
The term Federal law enforcement assistance is defined by the Act to mean funds, equipment, training, intelligence information, and personnel.

(c) Federal law enforcement community.
The term Federal law enforcement community is defined by the Act as the heads of the following departments or agencies:

(1) Federal Bureau of Investigation;
(2) Drug Enforcement Administration;
(3) Criminal Division of the Department of Justice;
(4) Internal Revenue Service;
(5) Customs Service;
(6) Department of Homeland Security;
(7) U.S. Marshals Service;
(8) National Park Service;
(9) U.S. Postal Service;
(10) Secret Service;
(11) U.S. Coast Guard;
(12) Bureau of Alcohol, Tobacco, Firearms, and Explosives;

(13) National Security Division of the Department of Justice; and

(14) Other Federal agencies with specific statutory authority to investigate violations of Federal criminal law.

(d) State.
The term state is defined by the Act as any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Trust Territory of the Pacific Islands, or the Commonwealth of the Northern Mariana Islands.

Official Citation:
SUBPART I—Immigration Emergency Fund

Source:
Order No. 1892-94, 59 FR 30522, June 14, 1994, unless otherwise noted.

28 CFR Section 65.80: General.

The regulations of this subpart set forth procedures for implementing section 404(b) of the Immigration and Nationality Act (“INA”), 8 U.S.C. 1101 note, by providing for Presidential determinations of the existence of an immigration emergency, and for payments from the Immigration Emergency Fund or other funding available for such purposes, to State and local governments for assistance provided in meeting an immigration emergency. The regulations of this subpart also establish procedures by which the Attorney General may draw upon the Immigration Emergency Fund, without a Presidential determination that an immigration emergency exists, to provide funding to State and local governments for assistance provided as required by the Attorney General in certain specified circumstances.

Official Citation:

28 CFR Section 65.81: General definitions.

As used in this part:

Assistance
means any actions taken by a State or local government directly relating to aiding the Attorney General in the administration of the immigration laws of the United States and in meeting urgent demands arising from the presence of aliens in the State or local government’s jurisdiction, when such actions are taken to assist in meeting an immigration emergency or under any of the circumstances specified in section 404(b)(2)(A) of the INA. Assistance may include, but need not be limited to, the provision of large shelter facilities for the housing and screening of aliens, and, in connection with these activities, the provision of such basic necessities as food, water clothing, and health care.

Immigration emergency
means an actual or imminent influx of aliens which either is of such magnitude or exhibits such other characteristics that effective administration of the
immigration laws of the United States is beyond the existing capabilities of the
Immigration and Naturalization Service ("INS") in the affected area or areas.
Characteristics of an influx of aliens, other than magnitude, which may be
considered in determining whether an immigration emergency exists include:
the likelihood of continued growth in the magnitude of the influx; an apparent
connection between the influx and increases in criminal activity; the actual or
imminent imposition of unusual and overwhelming demands on law enforcement
agencies; and other similar characteristics.

Other circumstances
means a situation that, as determined by the Attorney General, requires the
resources of a State or local government to ensure the proper administration of
the immigration laws of the United States or to meet urgent demands arising
from the presence of aliens in a State or local government's jurisdiction.

28 CFR Section 65.82: Procedure for requesting a Presidential
determination of an immigration emergency.

(a) The President may make a determination concerning the existence of an
immigration emergency after review of a request from either the Attorney
General of the United States or the chief executive of a State or local government.
Such a request shall include a description of the facts believed to constitute an
immigration emergency and the types of assistance needed to meet that
emergency. Except when a request is made by the Attorney General, the
requestor shall file the original application with the Office of the President and
shall file copies of the application with the Attorney General and with the
Commissioner of INS.

(b) If the President determines that an immigration emergency exists, the
President shall certify that fact to the Judiciary Committees of the House of
Representatives and of the Senate.

28 CFR Section 65.83: Assistance required by the Attorney
General.

The Attorney General may request assistance from a State or local government in
the administration of the immigration laws of the United States or in meeting
urgent demands where the need for assistance arises because of the presence of
aliens in that State or local jurisdiction, and may provide funding to a State or
local government relating to such assistance from the Immigration Emergency
Fund or other funding available for such purposes, without a Presidential
determination of an immigration emergency, in any of the following circumstances:

(a) An INS district director certifies to the Commissioner of INS, who shall, in turn, certify to the Attorney General, that the number of asylum applications filed in that INS district during the relevant calendar quarter exceeds by at least 1,000 the number of such applications filed in that district during the preceding calendar quarter. For purposes of this paragraph, providing parole at a point of entry in a district shall be deemed to constitute an application for asylum in the district.

(b) The Attorney General determines that there exist circumstances involving the administration of the immigration laws of the United States that endanger the lives, property, safety, or welfare of the residents of a State or locality.

(c) The Attorney General determines that there exist any other circumstances, as defined in § 65.81 of this subpart, such that it is appropriate to seek assistance from a State or local government in administering the immigration laws of the United States or in meeting urgent demands arising from the presence of aliens in a State or local jurisdiction.

(d)(1) If, in making a determination pursuant to paragraph (b) or (c) of this section, the Attorney General also determines that the situation involves an actual or imminent mass influx of aliens arriving off the coast or near a land border of the United States and presents urgent circumstances requiring an immediate Federal response, the Attorney General will formally declare that a mass influx of aliens is imminent or occurring. The determination that a mass influx of aliens is imminent or occurring will be based on the factors set forth in the definitions contained in § 65.81 of this subpart. The Attorney General will determine and define the time period that encompasses a mass influx of aliens by declaring when such an event begins and when it ends. The Attorney General will initially define the geographic boundaries where the mass influx of aliens is imminent or occurring.

(2) Based on evolving developments in the scope of the event, the Commissioner of the INS may, as necessary, amend and redefine the geographic area defined by the Attorney General to expand or decrease the boundaries. This authority shall not be further delegated.

(3) The Attorney General, pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), may authorize any State or local law enforcement officer to perform or exercise any of the powers, privileges, or duties conferred or imposed by the Act, or regulations issued thereunder, upon officers or employees of the Service. Such authorization must be with the consent of the head of the
department, agency, or establishment under whose jurisdiction the officer is serving.

(4) Authorization for State or local law enforcement officers to exercise Federal immigration law enforcement authority for transporting or guarding aliens in custody may be exercised as necessary beyond the defined geographic boundaries where the mass influx of aliens is imminent or occurring. Otherwise, Federal immigration law enforcement authority to be exercised by State or local law enforcement officers will be authorized only within the defined geographic boundaries where the mass influx of aliens is imminent or occurring.

(5) State or local law enforcement officers will be authorized to exercise Federal immigration law enforcement authority only during the time period prescribed by the Attorney General in conjunction with the initiation and termination of a declared mass influx of aliens.

Official Citation:

28 CFR Section 65.84: Procedures for the Attorney General when seeking State or local assistance.

(a)(1) When the Attorney General determines to seek assistance from a State or local government under § 65.83 of this subpart, or when the President has determined that an immigration emergency exists, the Attorney General shall negotiate the terms and conditions of that assistance with the State or local government. The Attorney General shall then execute a written agreement with appropriate State or local officials, which sets forth the terms and conditions of the assistance, including funding. Such written agreements can be reimbursement agreements, grants, or cooperative agreements.

(2) The Commissioner may execute written contingency agreements regarding assistance under § 65.83(d) of this subpart in advance of the Attorney General’s determination pursuant to that section. However, such advance agreements shall not authorize State or local law enforcement officers to perform any functions of Service officers or employees under section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), until the Attorney General has made the necessary determinations and authorizes such performance. Any such advance agreements shall contain precise activation procedures.

(3) Written agreements regarding assistance under § 65.83(d) of this subpart, including contingency agreements, shall include the following minimum requirements:
(i) A statement of the powers, privileges, or duties that State or local law enforcement officers will be authorized to exercise and the conditions under which they may be exercised;

(ii) A statement of the types of assistance by State or local law enforcement officers for which the Attorney General shall be responsible for reimbursing the relevant parties in accordance with the procedures set forth in paragraph (b) of this section;

(iii) A statement that the relevant State or local law enforcement officers are not authorized to exercise any functions of Service officers or employees under section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), until the Attorney General has made a determination pursuant to that section and authorizes such performance;

(iv) A requirement that State or local law enforcement officers cannot exercise any authorized functions of Service officers or employees under section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), until they have successfully completed and been certified in a Service-prescribed course of instruction in basic immigration law, immigration law enforcement fundamentals and procedures, civil rights law, and sensitivity and cultural awareness issues;

(v) A description of the duration of the written agreement, and of the authority the Attorney General will confer upon State or local law enforcement officers pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), along with a provision for amending, terminating, or extending the duration of the written agreement, or for terminating or amending the authority to be conferred pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8);

(vi) A requirement that the exercise of any Service officer functions by State or local law enforcement officers pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), be at the direction of the Service;

(vii) A requirement that any State or local law enforcement officer performing Service officer or employee functions pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), must adhere to the policies and standards set forth during the training, including applicable immigration law enforcement standards and procedures, civil rights law, and sensitivity and cultural awareness issues;

(viii) A statement that the authority to perform Service officer or employee functions pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), does not abrogate or abridge constitutional or civil rights protections;
(ix) A requirement that a complaint reporting and resolution procedure for allegations of misconduct or wrongdoing by State or local officers designated, or activities undertaken, pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), be in place;

(x) A requirement that a mechanism to record and monitor complaints regarding the immigration enforcement activities of State or local law enforcement officers authorized to enforce immigration laws be in place;

(xi) A listing by position (title and name when available) of the Service officers authorized to provide operational direction to State or local law enforcement officers assisting in a Federal response pursuant to section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8);

(xii) A requirement that a State or local law enforcement agency maintain records of operational expenditures incurred as a result of supporting the Federal response to a mass influx of aliens;

(xiii) Provisions concerning State or local law enforcement officer use of Federal property or facilities, if any;

(xiv) A requirement that any department, agency, or establishment whose State or local law enforcement officer is performing Service officer or employee functions shall cooperate fully in any Federal investigation related to allegations of misconduct or wrongdoing in conjunction with such functions, or to the written agreement; and

(xv) A procedure by which the appropriate law enforcement agency, department, or establishment will be notified that the Attorney General has made a determination under section 103(a)(8) of the INA, 8 U.S.C. 1103(a)(8), to authorize State or local law enforcement officers to exercise Federal immigration enforcement authority under the provisions of the respective agreements.

(4) The Attorney General may abbreviate or waive any of the training required pursuant to a written agreement regarding assistance under § 65.83(d) of this chapter, including contingency agreements, in the event that the number of State or local law enforcement officers available to respond in an expeditious manner to urgent and quickly developing events during a declared mass influx of aliens is insufficient to protect public safety, public health, or national security. Such officers still would be required to adhere to applicable policies and standards of the Immigration and Naturalization Service. The decision to abbreviate or waive these training requirements is at the sole discretion of the Attorney General.

(b) A reimbursement agreement shall contain the procedures under which the State or local government is to obtain reimbursement for its assistance. A
reimbursement agreement shall include the title of the official to whom claims are to be submitted, the intervals at which claims are to be submitted, a description of the supporting documentation to be submitted, and any limitations on the total amount of reimbursement that will be provided. Grants and cooperative agreements shall be made and administered in accordance with the uniform procedures in part 66 of this title.

(c) In exigent circumstances, the Attorney General may agree to provide funding to a State or local government without a written agreement. A reimbursement agreement, grant, or cooperative agreement conforming to the specifications in this section shall be reduced to writing as soon as practicable.

**Official Citation:**

28 CFR Section 65.85: Procedures for State or local governments applying for funding.

(a) In the event that the chief executive of a State or local government determines that any of the circumstances set forth in § 65.83 of this subpart exists, he or she may pursue the procedures in this section to submit to the Attorney General an application for a reimbursement agreement, grant, or cooperative agreement as described in § 65.84 of this subpart.

(b) The Department strongly encourages chief executives of States and local governments, if possible, to consult informally with the Attorney General and the Commissioner of INS prior to submitting a formal application. This informal consultation is intended to facilitate discussion of the nature of the assistance to be provided by the State or local government, the requirements of the Attorney General, if any, for such assistance, the costs associated with such assistance, and the Department’s preliminary views on the appropriateness of the proposed funding.

(c) The chief executive of a State or local government shall submit an application in writing to the Attorney General, and shall file a copy with the Commissioner of INS. The application shall set forth in detail the following information:

(1) The name of the jurisdiction requesting reimbursement;

(2) All facts supporting the application;
(3) The nature of the assistance which the State or local government has provided or will provide, as required by the Attorney General, for which funding is requested;

(4) The dollar amount of the funding sought;

(5) A justification for the amount of funding being sought;

(6) The expected duration of the conditions requiring State or local assistance;

(7) Information about whether funding is sought for past costs or for future costs;

(8) The name, address, and telephone number of a contact person from the requesting jurisdiction.

(d) If the Attorney General determines that the assistance for which funding is sought under paragraph (c) of this section is appropriate under the standards of this subpart, the Attorney General may enter into a reimbursement or cooperative agreement or may make a grant in the same manner as if the assistance had been requested by the Attorney General as described under § 65.84 of this subpart.

(e) The Attorney General will consider all applications from State or local governments until the Attorney General has obligated funding available for such purposes as determined by the Attorney General. The Attorney General will make a decision with respect to any application submitted under this section that contains the information described in paragraph (c) of this section within 15 calendar days of such application.

(f) In exigent circumstances, the Attorney General may waive the requirements of this section concerning the form, contents, and order of consideration of applications, including the requirement in paragraph (c) of this section that applications be submitted in writing.

Official Citation:
28 CFR PART 69—NEW RESTRICTIONS ON LOBBYING

- Subpart A—General
  - 28 CFR Section 69.100: Conditions on use of funds.
  - 28 CFR Section 69.105: Definitions.
  - 28 CFR Section 69.110: Certification and disclosure.
- Subpart B—Activities by Own Employees
  - 28 CFR Section 69.200: Agency and legislative liaison.
  - 28 CFR Section 69.205: Professional and technical services.
  - 28 CFR Section 69.210: Reporting.
- Subpart C—Activities by Other Than Own Employees
  - 28 CFR Section 69.300: Professional and technical services.
- Subpart D—Penalties and Enforcement
  - 28 CFR Section 69.400: Penalties.
  - 28 CFR Section 69.405: Penalty procedures.
  - 28 CFR Section 69.410: Enforcement.
- Subpart E—Exemptions
  - 28 CFR Section 69.500: Secretary of Defense.
- Subpart F—Agency Reports
  - 28 CFR Section 69.600: Semi-annual compilation.
- Appendix A to Part 69—Certification Regarding Lobbying
- Appendix B to Part 69—Disclosure Form To Report Lobbying

Authority:
Sec. 319, Public Law 101-121 (31 U.S.C. 1352); [citation to Agency rulemaking authority].

Cross Reference:
See also Office of Management and Budget notice published at 54 FR 52306, December 20, 1989.

Source:
55 FR 6737, 6751, Feb. 26, 1990, unless otherwise noted.
(a) No appropriated funds may be expended by the recipient of a Federal contract, grant, loan, or cooperative agreement to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered Federal actions: the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(b) Each person who requests or receives from an agency a Federal contract, grant, loan, or cooperative agreement shall file with that agency a certification, set forth in appendix A, that the person has not made, and will not make, any payment prohibited by paragraph (a) of this section.

(c) Each person who requests or receives from an agency a Federal contract, grant, loan, or a cooperative agreement shall file with that agency a disclosure form, set forth in appendix B, if such person has made or has agreed to make any payment using nonappropriated funds (to include profits from any covered Federal action), which would be prohibited under paragraph (a) of this section if paid for with appropriated funds.

(d) Each person who requests or receives from an agency a commitment providing for the United States to insure or guarantee a loan shall file with that agency a statement, set forth in appendix A, whether that person has made or has agreed to make any payment to influence or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with that loan insurance or guarantee.

(e) Each person who requests or receives from an agency a commitment providing for the United States to insure or guarantee a loan shall file with that agency a disclosure form, set forth in appendix B, if that person has made or has agreed to make any payment to influence or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with that loan insurance or guarantee.

28 CFR Section 69.105: Definitions.
For purposes of this part:

(a) Agency, as defined in 5 U.S.C. 552(f), includes Federal executive departments and agencies as well as independent regulatory commissions and Government corporations, as defined in 31 U.S.C. 9101(1).

(b) Covered Federal action means any of the following Federal actions:

(1) The awarding of any Federal contract;

(2) The making of any Federal grant;

(3) The making of any Federal loan;

(4) The entering into of any cooperative agreement; and,

(5) The extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

Covered Federal action does not include receiving from an agency a commitment providing for the United States to insure or guarantee a loan. Loan guarantees and loan insurance are addressed independently within this part.

(c) Federal contract means an acquisition contract awarded by an agency, including those subject to the Federal Acquisition Regulation (FAR), and any other acquisition contract for real or personal property or services not subject to the FAR.

(d) Federal cooperative agreement means a cooperative agreement entered into by an agency.

(e) Federal grant means an award of financial assistance in the form of money, or property in lieu of money, by the Federal Government or a direct appropriation made by law to any person. The term does not include technical assistance which provides services instead of money, or other assistance in the form of revenue sharing, loans, loan guarantees, loan insurance, interest subsidies, insurance, or direct United States cash assistance to an individual.

(f) Federal loan means a loan made by an agency. The term does not include loan guarantee or loan insurance.

(g) Indian tribe and tribal organization
have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450B). Alaskan Natives are included under the definitions of Indian tribes in that Act.

(h) Influencing or attempting to influence means making, with the intent to influence, any communication to or appearance before an officer or employee or any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal action.

(i) Loan guarantee and loan insurance means an agency's guarantee or insurance of a loan made by a person.

(j) Local government means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

(k) Officer or employee of an agency includes the following individuals who are employed by an agency:

(1) An individual who is appointed to a position in the Government under title 5, U.S. Code, including a position under a temporary appointment;

(2) A member of the uniformed services as defined in section 101(3), title 37, U.S. Code;

(3) A special Government employee as defined in section 202, title 18, U.S. Code; and,

(4) An individual who is a member of a Federal advisory committee, as defined by the Federal Advisory Committee Act, title 5, U.S. Code appendix 2.

(l) Person means an individual, corporation, company, association, authority, firm, partnership, society, State, and local government, regardless of whether such entity is operated for profit or not for profit. This term excludes an Indian tribe, tribal organization, or any other Indian organization with respect to expenditures specifically permitted by other Federal law.

(m) Reasonable compensation means, with respect to a regularly employed officer or employee of any person, compensation that is consistent with the normal compensation for such officer or
employee for work that is not furnished to, not funded by, or not furnished in cooperation with the Federal Government.

(n) Reasonable payment means, with respect to professional and other technical services, a payment in an amount that is consistent with the amount normally paid for such services in the private sector.

(o) Recipient includes all contractors, subcontractors at any tier, and subgrantees at any tier of the recipient of funds received in connection with a Federal contract, grant, loan, or cooperative agreement. The term excludes an Indian tribe, tribal organization, or any other Indian organization with respect to expenditures specifically permitted by other Federal law.

(p) Regularly employed means, with respect to an officer or employee of a person requesting or receiving a Federal contract, grant, loan, or cooperative agreement or a commitment providing for the United States to insure or guarantee a loan, an officer or employee who is employed by such person for at least 130 working days within one year immediately preceding the date of the submission that initiates agency consideration of such person for receipt of such contract, grant, loan, cooperative agreement, loan insurance commitment, or loan guarantee commitment. An officer or employee who is employed by such person for less than 130 working days within one year immediately preceding the date of the submission that initiates agency consideration of such person shall be considered to be regularly employed as soon as he or she is employed by such person for 130 working days.

(q) State means a State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, a territory or possession of the United States, an agency or instrumentality of a State, and a multi-State, regional, or interstate entity having governmental duties and powers.

28 CFR Section 69.110: Certification and disclosure.

(a) Each person shall file a certification, and a disclosure form, if required, with each submission that initiates agency consideration of such person for:

(1) Award of a Federal contract, grant, or cooperative agreement exceeding $100,000; or

(2) An award of a Federal loan or a commitment providing for the United States to insure or guarantee a loan exceeding $150,000.
(b) Each person shall file a certification, and a disclosure form, if required, upon receipt by such person of:

(1) A Federal contract, grant, or cooperative agreement exceeding $100,000; or

(2) A Federal loan or a commitment providing for the United States to insure or guarantee a loan exceeding $150,000,

Unless such person previously filed a certification, and a disclosure form, if required, under paragraph (a) of this section.

(c) Each person shall file a disclosure form at the end of each calendar quarter in which there occurs any event that requires disclosure or that materially affects the accuracy of the information contained in any disclosure form previously filed by such person under paragraphs (a) or (b) of this section. An event that materially affects the accuracy of the information reported includes:

(1) A cumulative increase of $25,000 or more in the amount paid or expected to be paid for influencing or attempting to influence a covered Federal action; or

(2) A change in the person(s) or individual(s) influencing or attempting to influence a covered Federal action; or,

(3) A change in the officer(s), employee(s), or Member(s) contacted to influence or attempt to influence a covered Federal action.

(d) Any person who requests or receives from a person referred to in paragraphs (a) or (b) of this section:

(1) A subcontract exceeding $100,000 at any tier under a Federal contract;

(2) A subgrant, contract, or subcontract exceeding $100,000 at any tier under a Federal grant;

(3) A contract or subcontract exceeding $100,000 at any tier under a Federal loan exceeding $150,000; or,

(4) A contract or subcontract exceeding $100,000 at any tier under a Federal cooperative agreement,

Shall file a certification, and a disclosure form, if required, to the next tier above.
(e) All disclosure forms, but not certifications, shall be forwarded from tier to tier until received by the person referred to in paragraphs (a) or (b) of this section. That person shall forward all disclosure forms to the agency.

(f) Any certification or disclosure form filed under paragraph (e) of this section shall be treated as a material representation of fact upon which all receiving tiers shall rely. All liability arising from an erroneous representation shall be borne solely by the tier filing that representation and shall not be shared by any tier to which the erroneous representation is forwarded. Submitting an erroneous certification or disclosure constitutes a failure to file the required certification or disclosure, respectively. If a person fails to file a required certification or disclosure, the United States may pursue all available remedies, including those authorized by section 1352, title 31, U.S. Code.

(g) For awards and commitments in process prior to December 23, 1989, but not made before that date, certifications shall be required at award or commitment, covering activities occurring between December 23, 1989, and the date of award or commitment. However, for awards and commitments in process prior to the December 23, 1989 effective date of these provisions, but not made before December 23, 1989, disclosure forms shall not be required at time of award or commitment but shall be filed within 30 days.

(h) No reporting is required for an activity paid for with appropriated funds if that activity is allowable under either subpart B or C.
SUBPART B—Activities by Own Employees
28 CFR Section 69.200: Agency and legislative liaison.

(a) The prohibition on the use of appropriated funds, in § 69.100 (a), does not apply in the case of a payment of reasonable compensation made to an officer or employee of a person requesting or receiving a Federal contract, grant, loan, or cooperative agreement if the payment is for agency and legislative liaison activities not directly related to a covered Federal action.

(b) For purposes of paragraph (a) of this section, providing any information specifically requested by an agency or Congress is allowable at any time.

(c) For purposes of paragraph (a) of this section, the following agency and legislative liaison activities are allowable at any time only where they are not related to a specific solicitation for any covered Federal action:

(1) Discussing with an agency (including individual demonstrations) the qualities and characteristics of the person's products or services, conditions or terms of sale, and service capabilities; and,

(2) Technical discussions and other activities regarding the application or adaptation of the person's products or services for an agency's use.

(d) For purposes of paragraph (a) of this section, the following agencies and legislative liaison activities are allowable only where they are prior to formal solicitation of any covered Federal action:

(1) Providing any information not specifically requested but necessary for an agency to make an informed decision about initiation of a covered Federal action;

(2) Technical discussions regarding the preparation of an unsolicited proposal prior to its official submission; and,

(3) Capability presentations by persons seeking awards from an agency pursuant to the provisions of the Small Business Act, as amended by Public Law 95-507 and other subsequent amendments.

(e) Only those activities expressly authorized by this section are allowable under this section.

28 CFR Section 69.205: Professional and technical services.
(a) The prohibition on the use of appropriated funds, in § 69.100 (a), does not apply in the case of a payment of reasonable compensation made to an officer or employee of a person requesting or receiving a Federal contract, grant, loan, or cooperative agreement or an extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement if payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal contract, grant, loan, or cooperative agreement or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal contract, grant, loan, or cooperative agreement.

(b) For purposes of paragraph (a) of this section, “professional and technical services” shall be limited to advice and analysis directly applying any professional or technical discipline. For example, drafting of a legal document accompanying a bid or proposal by a lawyer is allowable. Similarly, technical advice provided by an engineer on the performance or operational capability of a piece of equipment rendered directly in the negotiation of a contract is allowable. However, communications with the intent to influence made by a professional (such as a licensed lawyer) or a technical person (such as a licensed accountant) are not allowable under this section unless they provide advice and analysis directly applying their professional or technical expertise and unless the advice or analysis is rendered directly and solely in the preparation, submission or negotiation of a covered Federal action. Thus, for example, communications with the intent to influence made by a lawyer that do not provide legal advice or analysis directly and solely related to the legal aspects of his or her client's proposal, but generally advocate one proposal over another are not allowable under this section because the lawyer is not providing professional legal services. Similarly, communications with the intent to influence made by an engineer providing an engineering analysis prior to the preparation or submission of a bid or proposal are not allowable under this section since the engineer is providing technical services but not directly in the preparation, submission or negotiation of a covered Federal action.

(c) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation, or reasonably expected to be required by law or regulation, and any other requirements in the actual award documents.

(d) Only those services expressly authorized by this section are allowable under this section.

28 CFR Section 69.210: Reporting.

No reporting is required with respect to payments of reasonable compensation made to regularly employed officers or employees of a person.
SUBPART C—Activities by Other Than Own Employees
28 CFR Section 69.300: Professional and technical services.

(a) The prohibition on the use of appropriated funds, in § 69.100 (a), does not apply in the case of any reasonable payment to a person, other than an officer or employee of a person requesting or receiving a covered Federal action, if the payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal contract, grant, loan, or cooperative agreement or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal contract, grant, loan, or cooperative agreement.

(b) The reporting requirements in § 69.110 (a) and (b) regarding filing a disclosure form by each person, if required, shall not apply with respect to professional or technical services rendered directly in the preparation, submission, or negotiation of any commitment providing for the United States to insure or guarantee a loan.

(c) For purposes of paragraph (a) of this section, “professional and technical services” shall be limited to advice and analysis directly applying any professional or technical discipline. For example, drafting or a legal document accompanying a bid or proposal by a lawyer is allowable. Similarly, technical advice provided by an engineer on the performance or operational capability of a piece of equipment rendered directly in the negotiation of a contract is allowable. However, communications with the intent to influence made by a professional (such as a licensed lawyer) or a technical person (such as a licensed accountant) are not allowable under this section unless they provide advice and analysis directly applying their professional or technical expertise and unless the advice or analysis is rendered directly and solely in the preparation, submission or negotiation of a covered Federal action. Thus, for example, communications with the intent to influence made by a lawyer that do not provide legal advice or analysis directly and solely related to the legal aspects of his or her client's proposal, but generally advocate one proposal over another are not allowable under this section because the lawyer is not providing professional legal services. Similarly, communications with the intent to influence made by an engineer providing an engineering analysis prior to the preparation or submission of a bid or proposal are not allowable under this section since the engineer is providing technical services but not directly in the preparation, submission or negotiation of a covered Federal action.

(d) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation, or reasonably expected to be required by law or regulation, and any other requirements in the actual award documents.

(e) Persons other than officers or employees of a person requesting or receiving a covered Federal action include consultants and trade associations.

(f) Only those services expressly authorized by this section are allowable under this section.

Page 807
SUBPART D—Penalties and Enforcement
28 CFR Section 69.400: Penalties.

(a) Any person who makes an expenditure prohibited herein shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such expenditure.

(b) Any person who fails to file or amend the disclosure form (see appendix B) to be filed or amended if required herein, shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

(c) A filing or amended filing on or after the date on which an administrative action for the imposition of a civil penalty is commenced does not prevent the imposition of such civil penalty for a failure occurring before that date. An administrative action is commenced with respect to a failure when an investigating official determines in writing to commence an investigation of an allegation of such failure.

(d) In determining whether to impose a civil penalty, and the amount of any such penalty, by reason of a violation by any person, the agency shall consider the nature, circumstances, extent, and gravity of the violation, the effect on the ability of such person to continue in business, any prior violations by such person, the degree of culpability of such person, the ability of the person to pay the penalty, and such other matters as may be appropriate.

(e) First offenders under paragraphs (a) or (b) of this section shall be subject to a civil penalty of $10,000, absent aggravating circumstances. Second and subsequent offenses by persons shall be subject to an appropriate civil penalty between $10,000 and $100,000, as determined by the agency head or his or her designee.

(f) An imposition of a civil penalty under this section does not prevent the United States from seeking any other remedy that may apply to the same conduct that is the basis for the imposition of such civil penalty.

28 CFR Section 69.405: Penalty procedures.

Agencies shall impose and collect civil penalties pursuant to the provisions of the Program Fraud and Civil Remedies Act, 31 U.S.C. sections 3803 (except subsection (c)), 3804, 3805, 3806, 3807, 3808, and 3812, insofar as these provisions are not inconsistent with the requirements herein.
28 CFR Section 69.410: Enforcement.

The head of each agency shall take such actions as are necessary to ensure that the provisions herein are vigorously implemented and enforced in that agency.
SUBPART E—Exemptions
28 CFR Section 69.500: Secretary of Defense.

(a) The Secretary of Defense may exempt, on a case-by-case basis, a covered Federal action from the prohibition whenever the Secretary determines, in writing, that such an exemption is in the national interest. The Secretary shall transmit a copy of each such written exemption to Congress immediately after making such a determination.

(b) The Department of Defense may issue supplemental regulations to implement paragraph (a) of this section.
SUBPART F—Agency Reports
28 CFR Section 69.600: Semi-annual compilation.

(a) The head of each agency shall collect and compile the disclosure reports (see appendix B) and, on May 31 and November 30 of each year, submit to the Secretary of the Senate and the Clerk of the House of Representatives a report containing a compilation of the information contained in the disclosure reports received during the six-month period ending on March 31 or September 30, respectively, of that year.

(b) The report, including the compilation, shall be available for public inspection 30 days after receipt of the report by the Secretary and the Clerk.

(c) Information that involves intelligence matters shall be reported only to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on Appropriations of the Senate and the House of Representatives in accordance with procedures agreed to by such committees. Such information shall not be available for public inspection.

(d) Information that is classified under Executive Order 12356 or any successor order shall be reported only to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives or the Committees on Armed Services of the Senate and the House of Representatives (whichever such committees have jurisdiction of matters involving such information) and to the Committees on Appropriations of the Senate and the House of Representatives in accordance with procedures agreed to by such committees. Such information shall not be available for public inspection.

(e) The first semi-annual compilation shall be submitted on May 31, 1990, and shall contain a compilation of the disclosure reports received from December 23, 1989 to March 31, 1990.

(f) Major agencies, designated by the Office of Management and Budget (OMB), are required to provide machine-readable compilations to the Secretary of the Senate and the Clerk of the House of Representatives no later than with the compilations due on May 31, 1991. OMB shall provide detailed specifications in a memorandum to these agencies.

(g) Non-major agencies are requested to provide machine-readable compilations to the Secretary of the Senate and the Clerk of the House of Representatives.

(h) Agencies shall keep the originals of all disclosure reports in the official files of the agency.
28 CFR Section 69.605: Inspector General report.

(a) The Inspector General, or other official as specified in paragraph (b) of this section, of each agency shall prepare and submit to Congress each year, commencing with submission of the President's Budget in 1991, an evaluation of the compliance of that agency with, and the effectiveness of, the requirements herein. The evaluation may include any recommended changes that may be necessary to strengthen or improve the requirements.

(b) In the case of an agency that does not have an Inspector General, the agency official comparable to an Inspector General shall prepare and submit the annual report, or, if there is no such comparable official, the head of the agency shall prepare and submit the annual report.

(c) The annual report shall be submitted at the same time the agency submits its annual budget justifications to Congress.

(d) The annual report shall include the following: All alleged violations relating to the agency's covered Federal actions during the year covered by the report, the actions taken by the head of the agency in the year covered by the report with respect to those alleged violations and alleged violations in previous years, and the amounts of civil penalties imposed by the agency in the year covered by the report.
Appendix A to Part 69—Certification Regarding Lobbying

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Statement for Loan Guarantees and Loan Insurance

The undersigned states, to the best of his or her knowledge and belief, that:

If any funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.
Submission of this statement is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.
28 CFR PART 73—NOTIFICATIONS TO THE ATTORNEY GENERAL BY AGENTS OF FOREIGN GOVERNMENTS

➢ 28 CFR Section 73.1: Definition of terms.
➢ 28 CFR Section 73.2: Exceptions.
➢ 28 CFR Section 73.3: Form of notification.
➢ 28 CFR Section 73.4: Partial compliance not deemed compliance.
➢ 28 CFR Section 73.5: Termination of notification.
➢ 28 CFR Section 73.6: Relation to other statutes.

Authority:

Source:
Order No. 1373-89, 54 FR 46608, Nov. 6, 1989, unless otherwise noted.
(a) The term agent means all individuals acting as representatives of, or on behalf
of, a foreign government or official, who are subject to the direction or control of
that foreign government or official, and who are not specifically excluded by the
terms of the Act or the regulations thereunder.

(b) The term foreign government includes any person or group of persons
exercising sovereign de facto or de jure political jurisdiction over any country,
other than the United States, or over any part of such country, and includes any
subdivision of any such group or agency to which such sovereign de facto or de
jure authority or functions are directly or indirectly delegated. Such term shall
include any faction or body of insurgents within a country assuming to exercise
governmental authority whether such faction or body of insurgents has or has not
been regarded by the United States as a governing authority.

(c) The term prior notification means the notification letter, telex, or facsimile
must be received by the addressee named in § 73.3 prior to commencing the
services contemplated by the parties.

(d) When used in 18 U.S.C. 951(d)(1), the term duly accredited means that the
sending State has notified the Department of State of the appointment and
arrival of the diplomatic or consular officer involved, and the Department of State
has not objected.

(e) When used in 18 U.S.C. 951(d)(2) and/or (3), the term officially and publicly
acknowledged and sponsored means that the person described therein has filed
with the Secretary of State a fully-executed notification of status with a foreign
government; or is a visitor, officially sponsored by a foreign government, whose
status is known and whose visit is authorized by an agency of the United States
Government; or is an official of a foreign government on a temporary visit to the
United States, for the purpose of conducting official business internal to the
affairs of that foreign government; or where an agent of a foreign government is
acting pursuant to the requirements of a Treaty, Executive Agreement,
Memorandum of Understanding, or other understanding to which the United
States or an agency of the United States is a party and which instrument
specifically establishes another mechanism for notification of visits by agents and
the terms of such visits.

(f) The term legal commercial transaction, for the purpose of 18 U.S.C. 951(d)(4),
means any exchange, transfer, purchase or sale, of any commodity, service or
property of any kind, including information or intellectual property, not
prohibited by federal or state legislation or implementing regulations.
28 CFR Section 73.2: Exceptions.

(a) The exemption provided in 18 U.S.C. 951(d)(4) for a “legal commercial transaction” shall not be available to any person acting subject to the direction or control of a foreign government or official where such person is an agent of Cuba or any other country that the President determines (and so reports to the Congress) poses a threat to the national security interest of the United States for purposes of 18 U.S.C. 951; or has been convicted of or entered a plea of nolo contendere to any offense under 18 U.S.C. 792-799, 831, or 2381, or under section 11 of the Export Administration Act of 1979, 50 U.S.C. app. 2410.

(b) The provisions of 18 U.S.C. 951(e)(2)(A) do not apply if the Attorney General, after consultation with the Secretary of State, determines and reports to Congress that the national security or foreign policy interests of the United States require that these provisions do not apply in specific circumstances to agents of such country.

(c) The provisions of 18 U.S.C. 951(e)(2)(B) do not apply to a person described in this clause for a period of more than five years beginning on the date of the conviction or the date of entry of the plea of nolo contendere.

Official Citation:

28 CFR Section 73.3: Form of notification.

(a) Notification shall be made by the agent in the form of a letter, telex, or facsimile addressed to the Attorney General, directed to the attention of the National Security Division, except for those agents described in paragraphs (b) and (c) of this section. The document shall state that it is a notification under 18 U.S.C. 951, and provide the name or names of the agent making the notification, the firm name, if any, and the business address or addresses of the agent, the identity of the foreign government or official for whom the agent is acting, and a brief description of the activities to be conducted for the foreign government or official and the anticipated duration of the activities. Each notification shall contain a certification, pursuant to 28 U.S.C. 1746, that the notification is true and correct.

(b) Notification by agents engaged in law enforcement investigations or regulatory agency activity shall be in the form of a letter, telex, or facsimile addressed to the Attorney General, directed to the attention of Interpol-United States National Central Bureau. Notification by agents engaged in intelligence,
counterintelligence, espionage, counterespionage or counterterrorism assignment or service shall be in the form of a letter, telex, or facsimile addressed to the Attorney General, directed to the attention of the nearest FBI Legal Attache. In case of exceptional circumstances, notification shall be provided contemporaneously or as soon as reasonably possible by the agent or the agent's supervisor. The letter, telex, or facsimile shall include the information set forth in paragraph (a) of this section.

(c) Notification made by agents engaged in judicial investigations pursuant to treaties or other mutual assistance requests or letters rogatory, shall be made in the form of a letter, telex, or facsimile addressed to the Attorney General, directed to the attention of the Office of International Affairs, Criminal Division. The letter, telex, or facsimile shall include the information set forth in paragraph (a) of this section.

(d) Any subsequent change in the information required by paragraph (a) of this section shall require a notification within 10 days of the change.

(e) Notification under 18 U.S.C. 951 shall be effective only if it has been done in compliance with this section, or if the agent has filed a registration under the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. 611, et seq., which provides the information required by paragraphs (a) and (d) of this section.

**Official Citation:**

**28 CFR Section 73.4: Partial compliance not deemed compliance.**

The fact that a notification has been filed shall not necessarily be deemed full compliance with 18 U.S.C. 951 or these regulations on the part of the agent; nor shall it indicate that the Attorney General has in any way passed on the merits of such notification or the legality of the agent's activities; nor shall it preclude prosecution, as provided for in 18 U.S.C. 951, for failure to file a notification when due, or for a false statement of a material fact therein, or for an omission of a material fact required to be stated therein.

**28 CFR Section 73.5: Termination of notification.**
(a) An agent shall, within 30 days after the termination of his agency relationship, advise the Attorney General of such change.

(b) All notifications pursuant to this part will automatically expire five years from the date of the most recent notification.

(c) An agent, whose notification expires pursuant to (b) above, must file a new notification within 10 days if the relationship continues.

28 CFR Section 73.6: Relation to other statutes.

The filing of a notification under this section shall not be deemed compliance with the requirements of the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. 611, et seq., nor compliance with any other statute.
28 CFR PART 77—ETHICAL STANDARDS FOR ATTORNEYS FOR THE GOVERNMENT

- 28 CFR Section 77.1: Purpose and authority.
- 28 CFR Section 77.2: Definitions.
- 28 CFR Section 77.3: Application of 28 U.S.C. 530B.
- 28 CFR Section 77.4: Guidance.
- 28 CFR Section 77.5: No private remedies.

Authority:
28 U.S.C. 530B.

Source:
Order No. 2216-99, 64 FR 19275, Apr. 20, 1999, unless otherwise noted.
28 CFR Section 77.1: Purpose and authority.

(a) The Department of Justice is committed to ensuring that its attorneys perform their duties in accordance with the highest ethical standards. The purpose of this part is to implement 28 U.S.C. 530B and to provide guidance to attorneys concerning the requirements imposed on Department attorneys by 28 U.S.C. 530B.

(b) Section 530B requires Department attorneys to comply with state and local federal court rules of professional responsibility, but should not be construed in any way to alter federal substantive, procedural, or evidentiary law or to interfere with the Attorney General's authority to send Department attorneys into any court in the United States.

(c) Section 530B imposes on Department attorneys the same rules of professional responsibility that apply to non-Department attorneys, but should not be construed to impose greater burdens on Department attorneys than those on non-Department attorneys or to alter rules of professional responsibility that expressly exempt government attorneys from their application.

(d) The regulations set forth in this part seek to provide guidance to Department attorneys in determining the rules with which such attorneys should comply.

28 CFR Section 77.2: Definitions.

As used in this part, the following terms shall have the following meanings, unless the context indicates otherwise:

(a) The phrase attorney for the government means the Attorney General; the Deputy Attorney General; the Solicitor General; the Assistant Attorneys General for, and any attorney employed in, the Antitrust Division, Civil Division, Civil Rights Division, Criminal Division, Environment and Natural Resources Division, and Tax Division; the Chief Counsel for the DEA and any attorney employed in that office; the Chief Counsel for ATF and any attorney employed in that office; the General Counsel of the FBI and any attorney employed in that office or in the (Office of General Counsel) of the FBI; any attorney employed in, or head of, any other legal office in a Department of Justice agency; any United States Attorney; any Assistant United States Attorney; any Special Assistant to the Attorney General or Special Attorney duly appointed pursuant to 28 U.S.C. 515; any Special Assistant United States Attorney duly appointed pursuant to 28 U.S.C. 543 who is authorized to conduct criminal or civil law enforcement investigations or proceedings on behalf of the United States; and any other attorney employed by the Department of Justice who is authorized to conduct criminal or civil law enforcement proceedings on behalf of the United States.
phrase attorney for the government also includes any independent counsel, or employee of such counsel, appointed under chapter 40 of title 28, United States Code. The phrase attorney for the government does not include attorneys employed as investigators or other law enforcement agents by the Department of Justice who are not authorized to represent the United States in criminal or civil law enforcement litigation or to supervise such proceedings.

(b) The term case means any proceeding over which a state or federal court has jurisdiction, including criminal prosecutions and civil actions. This term also includes grand jury investigations and related proceedings (such as motions to quash grand jury subpoenas and motions to compel testimony), applications for search warrants, and applications for electronic surveillance.

(c) The phrase civil law enforcement investigation means an investigation of possible civil violations of, or claims under, federal law that may form the basis for a civil law enforcement proceeding.

(d) The phrase civil law enforcement proceeding means a civil action or proceeding before any court or other tribunal brought by the Department of Justice under the authority of the United States to enforce federal laws or regulations, and includes proceedings related to the enforcement of an administrative subpoena or summons or civil investigative demand.

(e) The terms conduct and activity means any act performed by a Department attorney that implicates a rule governing attorneys, as that term is defined in paragraph (h) of this section.

(f) The phrase Department attorney[s] is synonymous with the phrase “attorney[s] for the government” as defined in this section.

(g) The term person means any individual or organization.

(h) The phrase state laws and rules and local federal court rules governing attorneys means rules enacted or adopted by any State or Territory of the United States or the District of Columbia or by any federal court, that prescribe ethical conduct for attorneys and that would subject an attorney, whether or not a Department attorney, to professional discipline, such as a code of professional responsibility. The phrase does not include:

1. Any statute, rule, or regulation which does not govern ethical conduct, such as rules of procedure, evidence, or substantive law, whether or not such rule is included in a code of professional responsibility for attorneys;
2. Any statute, rule, or regulation that purports to govern the conduct of any class of persons other than attorneys, such as rules that govern the conduct of all litigants and judges, as well as attorneys; or
3. A statute, rule, or regulation requiring licensure or membership in a particular state bar.
(i) The phrase state of licensure means the District of Columbia or any State or Territory where a Department attorney is duly licensed and authorized to practice as an attorney. This term shall be construed in the same manner as it has been construed pursuant to the provisions of Pub. L. 96-132, 93 Stat. 1040, 1044 (1979), and Sec. 102 of the Departments of Commerce, Justice and State, the Judiciary, and Related Agency Appropriations Act, 1999, Pub. L. 105-277.

(j)

(1) The phrase where such attorney engages in that attorney's duties identifies which rules of ethical conduct a Department attorney should comply with, and means, with respect to particular conduct:
   (i) If there is a case pending, the rules of ethical conduct adopted by the local federal court or state court before which the case is pending; or
   (ii) If there is no case pending, the rules of ethical conduct that would be applied by the attorney's state of licensure.

(2) A Department attorney does not “engage[] in that attorney's duties” in any states in which the attorney's conduct is not substantial and continuous, such as a jurisdiction in which an attorney takes a deposition (related to a case pending in another court) or directs a contact to be made by an investigative agent, or responds to an inquiry by an investigative agent. Nor does the phrase include any jurisdiction that would not ordinarily apply its rules of ethical conduct to particular conduct or activity by the attorney.

(k) The phrase to the same extent and in the same manner as other attorneys means that Department attorneys shall only be subject to laws and rules of ethical conduct governing attorneys in the same manner as such rules apply to non-Department attorneys. The phrase does not, however, purport to eliminate or otherwise alter state or federal laws and rules and federal court rules that expressly exclude some or all government attorneys from particular limitations or prohibitions.

Official Citation:

28 CFR Section 77.3: Application of 28 U.S.C. 530B.

In all criminal investigations and prosecutions, in all civil investigations and litigation (affirmative and defensive), and in all civil law enforcement investigations and proceedings, attorneys for the government shall conform their conduct and activities to the state rules and laws, and federal local court rules,
governing attorneys in each State where such attorney engages in that attorney's
duties, to the same extent and in the same manner as other attorneys in that
State, as these terms are defined in § 77.2 of this part.

28 CFR Section 77.4: Guidance.

(a) Rules of the court before which a case is pending.
A government attorney shall, in all cases, comply with the rules of ethical conduct
of the court before which a particular case is pending,

(b) Inconsistent rules where there is a pending case.
(1) If the rule of the attorney's state of licensure would prohibit an action
that is permissible under the rules of the court before which a case is pending, the
attorney should consider:

   (i) Whether the attorney's state of licensure would apply the rule of
   the court before which the case is pending, rather than the rule of the state of
   licensure;

   (ii) Whether the local federal court rule preempts contrary state
   rules; and

   (iii) Whether application of traditional choice-of-law principles
directs the attorney to comply with a particular rule.

(2) In the process of considering the factors described in paragraph (b)(1)
of this section, the attorney is encouraged to consult with a supervisor or
Professional Responsibility Officer to determine the best course of conduct.

(c) Choice of rules where there is no pending case.
(1) Where no case is pending, the attorney should generally comply with
the ethical rules of the attorney's state of licensure, unless application of
traditional choice-of-law principles directs the attorney to comply with the ethical
rule of another jurisdiction or court, such as the ethical rule adopted by the court
in which the case is likely to be brought.

(2) In the process of considering the factors described in paragraph (c)(1)
of this section, the attorney is encouraged to consult with a supervisor or
Professional Responsibility Officer to determine the best course of conduct.

(d) Rules that impose an irreconcilable conflict.
If, after consideration of traditional choice-of-law principles, the attorney
concludes that multiple rules may apply to particular conduct and that such rules

Page 826
impose irreconcilable obligations on the attorney, the attorney should consult with a supervisor or Professional Responsibility Officer to determine the best course of conduct.

(e) Supervisory attorneys. Each attorney, including supervisory attorneys, must assess his or her ethical obligations with respect to particular conduct. Department attorneys shall not direct any attorney to engage in conduct that violates section 530B. A supervisor or other Department attorney who, in good faith, gives advice or guidance to another Department attorney about the other attorney's ethical obligations should not be deemed to violate these rules.

(f) Investigative Agents. A Department attorney shall not direct an investigative agent acting under the attorney's supervision to engage in conduct under circumstances that would violate the attorney's obligations under section 530B. A Department attorney who in good faith provides legal advice or guidance upon request to an investigative agent should not be deemed to violate these rules.

28 CFR Section 77.5: No private remedies. The principles set forth herein, and internal office procedures adopted pursuant hereto, are intended solely for the guidance of attorneys for the government. They are not intended to, do not, and may not be relied upon to create a right or benefit, substantive or procedural, enforceable at law by a party to litigation with the United States, including criminal defendants, targets or subjects of criminal investigations, witnesses in criminal or civil cases (including civil law enforcement proceedings), or plaintiffs or defendants in civil investigations or litigation; or any other person, whether or not a party to litigation with the United States, or their counsel; and shall not be a basis for dismissing criminal or civil charges or proceedings or for excluding relevant evidence in any judicial or administrative proceeding. Nor are any limitations placed on otherwise lawful litigative prerogatives of the Department of Justice as a result of this part.
28 CFR PART 80—FOREIGN CORRUPT PRACTICES ACT OPINION PROCEDURE

➤ 28 CFR Section 80.1: Purpose.
➤ 28 CFR Section 80.2: Submission requirements.
➤ 28 CFR Section 80.3: Transaction.
➤ 28 CFR Section 80.4: Issuer or domestic concern.
➤ 28 CFR Section 80.5: Affected parties.
➤ 28 CFR Section 80.6: General requirements.
➤ 28 CFR Section 80.7: Additional information.
➤ 28 CFR Section 80.8: Attorney General opinion.
➤ 28 CFR Section 80.9: No oral opinion.
➤ 28 CFR Section 80.10: Rebuttable presumption.
➤ 28 CFR Section 80.11: Effect of FCPA Opinion.
➤ 28 CFR Section 80.12: Accounting requirements.
➤ 28 CFR Section 80.13: Scope of FCPA Opinion.
➤ 28 CFR Section 80.14: Disclosure.
➤ 28 CFR Section 80.15: Withdrawal.
➤ 28 CFR Section 80.16: Additional requests.

Authority:

Source:
Order No. 1620-92, 57 FR 39600, Sept. 1, 1992, unless otherwise noted.
28 CFR Section 80.1: Purpose.

These procedures enable issuers and domestic concerns to obtain an opinion of the Attorney General as to whether certain specified, prospective—not hypothetical—conduct conforms with the Department’s present enforcement policy regarding the antibribery provisions of the Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. 78dd-1 and 78dd-2. An opinion issued pursuant to these procedures is a Foreign Corrupt Practices Act opinion (hereinafter FCPA Opinion).

28 CFR Section 80.2: Submission requirements.

A request for an FCPA Opinion must be submitted in writing. An original and five copies of the request should be addressed to the Assistant Attorney General in charge of the Criminal Division, Attention: FCPA Opinion Group. The mailing address is P.O. Box 28188, Central Station, Washington, DC 20038. The address for hand delivery is room 2424, Bond Building, 1400 New York Avenue, NW., Washington, DC 20005.

28 CFR Section 80.3: Transaction.

The entire transaction which is the subject of the request must be an actual—not a hypothetical—transaction but need not involve only prospective conduct. However, a request will not be considered unless that portion of the transaction for which an opinion is sought involves only prospective conduct. An executed contract is not a prerequisite and, in most—if not all—instances, an opinion request should be made prior to the requestor’s commitment to proceed with a transaction.

28 CFR Section 80.4: Issuer or domestic concern.

The request must be submitted by an issuer or domestic concern within the meaning of 15 U.S.C. 78dd-1 and 78dd-2, respectively, that is also a party to the transaction which is the subject of the request.

28 CFR Section 80.5: Affected parties.
An FCPA Opinion shall have no application to any party which does not join in the request for the opinion.

28 CFR Section 80.6: General requirements.

Each request shall be specific and must be accompanied by all relevant and material information bearing on the conduct for which an FCPA Opinion is requested and on the circumstances of the prospective conduct, including background information, complete copies of all operative documents, and detailed statements of all collateral or oral understandings, if any. The requesting issuer or domestic concern is under an affirmative obligation to make full and true disclosure with respect to the conduct for which an opinion is requested. Each request on behalf of a requesting issuer or corporate domestic concern must be signed by an appropriate senior officer with operational responsibility for the conduct that is the subject of the request and who has been designated by the requestor's chief executive officer to sign the opinion request. In appropriate cases, the Department of Justice may require the chief executive officer of each requesting issuer or corporate domestic concern to sign the request. All requests of other domestic concerns must also be signed. The person signing the request must certify that it contains a true, correct and complete disclosure with respect to the proposed conduct and the circumstances of the conduct.

28 CFR Section 80.7: Additional information.

If an issuer's or domestic concern's submission does not contain all of the information required by § 80.6, the Department of Justice may request whatever additional information or documents it deems necessary to review the matter. The Department must do so within 30 days of receipt of the opinion request, or, in the case of an incomplete response to a previous request for additional information, within 30 days of receipt of such response. Each issuer or domestic concern requesting an FCPA Opinion must promptly provide the information requested. A request will not be deemed complete until the Department of Justice receives such additional information. Such additional information, if furnished orally, shall be promptly confirmed in writing, signed by the same person or officer who signed the initial request and certified by this person or officer to be a true, correct and complete disclosure of the requested information. In connection with any request for an FCPA Opinion, the Department of Justice may conduct whatever independent investigation it believes appropriate.
28 CFR Section 80.8: Attorney General opinion.

The Attorney General or his designee shall, within 30 days after receiving a request that complies with the foregoing procedure, respond to the request by issuing an opinion that states whether the prospective conduct, would, for purposes of the Department of Justice's present enforcement policy, violate 15 U.S.C. 78dd-1 and 78dd-2. The Department of Justice may also take such other positions or action as it considers appropriate. Should the Department request additional information, the Department's response shall be made within 30 days after receipt of such additional information.

28 CFR Section 80.9: No oral opinion.

No oral clearance, release or other statement purporting to limit the enforcement discretion of the Department of Justice may be given. The requesting issuer or domestic concern may rely only upon a written FCPA Opinion letter signed by the Attorney General or his designee.

28 CFR Section 80.10: Rebuttable presumption.

In any action brought under the applicable provisions of 15 U.S.C. 78dd-1 and 78dd-2, there shall be a rebuttable presumption that a requestor's conduct, which is specified in a request, and for which the Attorney General has issued an opinion that such conduct is in conformity with the Department's present enforcement policy, is in compliance with those provisions of the FCPA. Such a presumption may be rebutted by a preponderance of the evidence. In considering the presumption, a court, in accordance with the statute, shall weigh all relevant factors, including but not limited to whether information submitted to the Attorney General was accurate and complete and whether the activity was within the scope of the conduct specified in any request received by the Attorney General.

28 CFR Section 80.11: Effect of FCPA Opinion.

Except as specified in § 80.10, an FCPA Opinion will not bind or obligate any agency other than the Department of Justice. It will not affect the requesting issuer's or domestic concern's obligations to any other agency, or under any statutory or regulatory provision other than those specifically cited in the particular FCPA Opinion.
28 CFR Section 80.12: Accounting requirements.

Neither the submission of a request for an FCPA Opinion, its pendency, nor the issuance of an FCPA Opinion, shall in any way alter the responsibility of an issuer to comply with the accounting requirements of 15 U.S.C. 78m(b)(2) and (3).

28 CFR Section 80.13: Scope of FCPA Opinion.

An FCPA Opinion will state only the Attorney General’s opinion as to whether the prospective conduct would violate the Department’s present enforcement policy under 15 U.S.C. 78dd-1 and 78dd-2. If the conduct for which an FCPA Opinion is requested is subject to approval by any other agency, such FCPA Opinion shall in no way be taken to indicate the Department of Justice’s views on the legal or factual issues that may be raised before that agency, or in an appeal from the agency’s decision.

28 CFR Section 80.14: Disclosure.

(a) Any document or other material which is provided to, received by, or prepared in the Department of Justice or any other department or agency of the United States in connection with a request by an issuer or domestic concern under the foregoing procedure shall be exempt from disclosure under 5 U.S.C. 552 and shall not, except with the consent of the issuer or domestic concern, be made publicly available, regardless of whether the Attorney General responds to such a request or the issuer or domestic concern withdrawal such request before receiving a response.

(b) Nothing contained in paragraph (a) of this section shall limit the Department of Justice’s right to issue, at its discretion, a release describing the identity of the requesting issuer or domestic concern, the identity of the foreign country in which the proposed conduct is to take place, the general nature and circumstances of the proposed conduct, and the action taken by the Department of Justice in response to the FCPA Opinion request. Such release shall not disclose either the identity of any foreign sales agents or other types of identifying information. The Department of Justice shall index such releases and place them in a file available to the public upon request.

(c) A requestor may request that the release not disclose proprietary information.
28 CFR Section 80.15: Withdrawal.

A request submitted under the foregoing procedure may be withdrawn prior to the time the Attorney General issues an opinion in response to such request. Any request so withdrawn shall have no force or effect. The Department of Justice reserves the right to retain any FCPA Opinion request, documents and information submitted to it under this procedure or otherwise and to use them for any governmental purposes, subject to the restrictions on disclosures in § 80.14.

28 CFR Section 80.16: Additional requests.

Additional requests for FCPA Opinions may be filed with the Attorney General under the foregoing procedure regarding other prospective conduct that is beyond the scope of conduct specified in previous requests.
28 CFR PART 100—COST RECOVERY REGULATIONS, COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994

- 28 CFR Section 100.9: General.
- 28 CFR Section 100.10: Definitions.
- 28 CFR Section 100.11: Allowable costs.
- 28 CFR Section 100.12: Reasonable costs.
- 28 CFR Section 100.13: Directly assignable costs.
- 28 CFR Section 100.14: Directly allocable costs.
- 28 CFR Section 100.15: Disallowed costs.
- 28 CFR Section 100.16: Cost estimate submission.
- 28 CFR Section 100.17: Request for payment.
- 28 CFR Section 100.18: Audit.
- 28 CFR Section 100.19: Adjustments to agreement estimate.
- 28 CFR Section 100.20: Confidentiality of trade secrets/proprietary information.
- 28 CFR Section 100.21: Alternative dispute resolution.

Authority:
47 U.S.C. 1001-1010; 28 CFR 0.85(o).

Source:
62 FR 13324, Mar. 20, 1997, unless otherwise noted.
28 CFR Section 100.9: General.

These Cost Recovery Regulations were developed to define allowable costs and establish reimbursement procedures in accordance with section 109(e) of Communications Assistance for Law Enforcement Act (CALEA) (Public Law 103-414, 108 Stat. 4279, 47 U.S.C. 1001-1010). Reimbursement of costs is subject to the availability of funds, the reasonableness of costs, and an agreement by the Attorney General or designee to reimburse costs prior to the carrier's incurrence of said costs.

28 CFR Section 100.10: Definitions.

Allocable means chargeable to one or more cost objectives and can be distributed to them in reasonable proportion to the benefits received.

Business unit means any segment of an organization for which cost data are routinely accumulated by the carrier for tracking and measurement purposes.

Cooperative agreement means the legal instrument reflecting a relationship between the government and a party when—

(1) The principal purpose of the relationship is to reimburse the carrier to carry out a public purpose of support or stimulation authorized by a law of the United States; and

(2) Substantial involvement is expected between the government and carrier when carrying out the activity contemplated in the agreement.

Cost element means a distinct component or category of costs (e.g. materials, direct labor, allocable direct costs, subcontracting costs, other costs) which is assigned to a cost objective.

Cost objective means a function, organizational subdivision, contract, or other work unit for which cost data are desired and for which provision is made to accumulate and measure the cost of processes, products, jobs, capitalized projects, etc.
Cost pool
means groupings of incurred costs identified with two or more cost objectives, but not identified specifically with any final cost objective.

Direct supervision
means immediate or first-level supervision.

Directly allocable cost
means any cost that is directly chargeable to one or more cost objectives and can be distributed to them in reasonable proportion to the benefits received.

Directly assignable cost
means any cost that can be wholly attributed to a cost objective.

Directly associated cost
means any directly assignable cost or directly allocable cost which is generated solely as a result of incurring another cost, and which would not have been incurred had the said cost not been incurred.

Final cost objective
means a cost objective that has allocated to it, both assignable and allocable costs and, in the carrier's accumulation system, is one of the final accumulation points.

Installed or deployed
means that, on a specific switching system, equipment, facilities, or services are operable and available for use by the carrier's customers.

Labor cost
means the sum of the payroll cost, payroll taxes, and directly associated benefits.

Network operations costs
means all directly associated costs related to the ongoing management and maintenance of a telecommunications carrier's network.

Plant costs
means the directly associated costs related to the modifications of specific kinds of telecommunications plants, such as switches, intelligent peripherals and other network elements. These costs shall include the costs of inspecting, testing and reporting on the condition of telecommunications plant to determine the need for replacements, rearranges and changes; rearranging and changing the location of plant not retired; inspecting after modifications have been made; the costs of modifying equipment records, such as administering trunking and circuit layout work; modifying operating procedures; property held for future telecommunications use; provisioning costs; network operations costs; and receiving training to perform plant work. Also included are the costs of direct supervision and office support of this work.

Provisioning costs
means all costs directly associated with the resources expended within a telecommunications carrier's network to provide a connection and/or service to an end user of the telecommunications service.

Trade secrets/proprietary information
means information which is in the possession of a carrier but not generally available to the public, which that carrier desires to protect against unrestricted disclosure or competitive use, and which is clearly identified as such at the time of its disclosure to the government.

Unit cost
means the directly associated cost of a single unit of a good or service which is included in a cost element.

28 CFR Section 100.11: Allowable costs.

(a) Costs that are eligible for reimbursement under section 109(e) CALEA are:

(1) All reasonable plant costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 103 of CALEA, until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modifications;

(2) Additional reasonable plant costs directly associated with making the assistance capability requirements found in section 103 of CALEA reasonably achievable with respect to equipment, facilities, or services installed or deployed
after January 1, 1995, in accordance with the procedures established in CALEA section 109(b); and

(3) Reasonable plant costs directly associated with modifications to any of a carrier's systems or services, as identified in the Carrier Statement required by CALEA section 104(d), that do not have the capacity to accommodate simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the Capacity Notice(s) published in accordance with CALEA section 104.

(b) Allowable plant costs shall include:

(1) The costs of installation, inspection, and testing of the telecommunications plant, and inspection after modifications have been made; and

(2) The costs of direct supervision and office support for this work for plant costs.

(c) In the case of any modification that may be used for any purpose other than lawfully authorized electronic surveillance by a government law enforcement agency, this part permits recovery of only the incremental cost of making the modification suitable for such law enforcement purposes.

(d) Reasonable costs that are directly associated with the modifications performed by a carrier as described in § 100.11(a) are recoverable. These allowable costs are limited to directly assignable and directly allocable costs incurred by the business units whose efforts are expended on the implementation of CALEA requirements.

28 CFR Section 100.12: Reasonable costs.

(a) A cost is reasonable if, in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of competitive business. Reasonableness of specific costs must be examined with particular care in connection with the carrier or its separate divisions that may not be subject to effective competitive restraints.

(1) No presumption of reasonableness shall be attached to the incurrence of costs by a carrier.

(2) The burden of proof shall be upon the carrier to justify that such cost is reasonable under this part.

Page 838
(b) Reasonableness depends upon considerations and circumstances, including, but not limited to:

(1) Whether a cost is of the type generally recognized as ordinary and necessary for the conduct of the carrier's business or the performance of this obligation; or

(2) Whether it is a generally accepted sound business practice, arm’s-length bargaining or the result of Federal or State laws and/or regulations.

(c) It is the carrier's responsibility to inform the Government of any deviation from the carrier's established practices.

28 CFR Section 100.13: Directly assignable costs.

(a) A cost is directly assignable to the CALEA compliance effort if it is a plant cost incurred specifically to meet the requirements of CALEA sections 103 and 104.

(1) A cost which has been incurred for the same purpose, in like circumstances, and which has been included in any allocable cost pool to be assigned to any final cost objective other than the CALEA compliance effort, shall not be assigned to the CALEA compliance effort (or any portion thereof).

(2) Costs identified specifically with the work performed are directly assignable costs to be charged directly to the CALEA compliance effort. All costs specifically identified with other projects, business units, or cost objectives of the carrier shall not be charged to the CALEA compliance effort, directly or indirectly.

(3) The burden of proof shall be upon the carrier to justify that such cost is an assignable cost under this part.

(b) For reasons of practicality, any directly assignable cost may be treated as a directly allocable cost if the accounting treatment is consistently applied within the carrier's accounting system and the application produces substantially the same results as treating the cost as a directly assignable cost.

28 CFR Section 100.14: Directly allocable costs.

(a) A cost is directly allocable to the CALEA compliance effort:
(1) If it is a plant cost incurred specifically to meet the requirements of CALEA sections 103 and 104; or

(2) If it benefits both the CALEA compliance effort and other work, and can be distributed to them in reasonable proportion to the benefits received.

(b) The burden of proof shall be upon the carrier to justify that such cost is an allocable cost under this part.

(c) An allocable cost shall not be assigned to the CALEA compliance effort if other costs incurred for the same purpose in like circumstances have been included as a direct cost of that, or any other, cost objective.

(d) The accumulation of allocable costs shall be as follows:

1. Allocable costs shall be accumulated by logical cost groupings with due consideration of the reasons for incurring such costs.

   (i) Each grouping should be determined so as to permit distribution of the grouping on the basis of the benefits accruing to the multiple cost objectives.

   (ii) Similarly, the particular case may require subdivision of these groupings (e.g., building occupancy costs might be separable from those of personnel administration within the engineering group).

2. Such allocation necessitates selecting a distribution base common to all cost objectives to which the grouping is to be allocated. The base should be selected so as to permit allocation of the grouping on the basis of the benefits accruing to the multiple cost objectives.

3. When substantially the same results can be achieved through less precise methods, the number and composition of cost groupings should be governed by practical considerations and should not unduly complicate the allocation.

4. Once a methodology for determining an appropriate base for distributing allocable costs has been agreed to, it shall not be modified without written approval of the FBI, if that modification affects the level of reimbursement from the government. All items properly includable in an allocable cost base should bear a pro rata share of allocable costs irrespective of their acceptance as reimbursable under this part.

5. The carrier's method of allocating allocable costs shall be in accordance with the accounting principles used by the carrier in the preparation of their
externally audited financial statements and consistently applied, to the extent that the expenses are allowable under there regulations. The method may require further examination when:

(i) Substantial differences occur between the cost patterns of work under CALEA compliance effort and the carrier's other work;

(ii) Significant changes occur in the nature of the business, the extent of subcontracting, fixed-asset improvement programs, inventories, the volume of sales and production, manufacturing processes, the carrier's products, or other relevant circumstances; or

(iii) Allocable cost groupings developed for a carrier's primary location are applied to off-site locations. Separate cost groupings for costs allocable to off-site locations may be necessary to permit equitable distribution of costs on the basis of the benefits accruing to the multiple cost objectives.

(6) The base period for allocating allocable costs is the cost accounting period during which such costs are incurred and accumulated for distribution to work performed in that period. The base period for allocating allocable costs will normally be the carrier's fiscal year. A shorter period may be appropriate when performance involves only a minor portion of the fiscal year, or when it is general practice to use a shorter period. When the compliance effort is performed over an extended period, as many base periods shall be used as are required to accurately represent the period of performance.

28 CFR Section 100.15: Disallowed costs.

(a) General and Administrative (G&A) costs are disallowed. G&A costs include, but are not limited to, any management, financial, and other expenditures which are incurred by or allocated to a business unit as a whole. These include, but are not limited to:

(1) Accounting and Finance, External Relations, Human Resources, Information Management, Legal, Procurement; and

(2) Other general administrative activities such as library services, food services, archives, and general security investigation services.

(b) Customer Service costs are disallowed. These costs include, but are not limited to, any Marketing, Sales, Product Management, and Advertising expenses.
(c) Plant costs that are not directly associated with the modifications identified in § 100.11 are disallowed. These include, but are not limited to, repairing materials for reuse, performing routine work to prevent trouble; expenses related to property held for future telecommunications use; provisioning costs; network operations costs; and depreciation and amortization expenses.

(d) Costs that have already been recovered from any governmental or nongovernmental entity are disallowed.

(e) Costs that cannot be either directly assigned or directly allocated are disallowed.

(f) Additional costs that are incurred due to the carrier's failure to complete the CALEA compliance effort in the time frame agreed to by the government and the carrier are disallowed.

(g) Costs associated with modifications of any equipment, facility or service installed or deployed after January 1, 1995 which are deemed reasonably achievable by the Federal Communications Commission under section 109(b) of CALEA are disallowed.

(h) To ensure that the Government does not reimburse carriers for disallowed costs, the following provisions are included:

1. Costs that are expressly disallowed or mutually agreed to be disallowed, including mutually agreed to be disallowed directly associated costs, shall be excluded from any billing, claim, or proposal applicable to reimbursement under CALEA. When a disallowed cost is incurred, its directly associated costs are also disallowed.

2. Disallowed costs involved in determining rates used for standard costs, or for allocable cost proposals or billing, need be identified only at the time rates are proposed, established, revised, or adjusted. These requirements may be satisfied by any form of cost identification which is adequate for purposes of cost determination and verification.

28 CFR Section 100.16: Cost estimate submission.

(a) The carrier shall provide sufficient cost data at the time of proposal submission to allow adequate analysis and evaluation of the estimated costs. The FBI reserves the right to request additional cost data from carriers in order to ensure compliance with this part.
(b) The requirement for submission of cost data is met if, as determined by the FBI, all cost data reasonably available to the carrier are either submitted or identified in writing by the date of agreement on the costs.

(c) If cost data and information to explain the estimating process are required by the FBI and the carrier refuses to provide necessary data, or the FBI determines that the data provided are so deficient as to preclude adequate analysis and evaluation, the FBI will attempt to obtain the data and/or elicit corrective action.

(d) Instructions for submission of the cost data for the estimate are as follows:

   (1) The carrier shall submit to the FBI estimated costs by line item with supporting information.

   (2) A cost element breakdown as described in § 100.16(h) shall be attached for each proposed line item.

   (3) Supporting breakdowns shall be furnished for each cost element, consistent with the carrier’s cost accounting system.

   (4) When more than one line item is proposed, summary total amounts covering all line items shall be furnished for each cost element.

   (5) Depending on the carrier’s accounting system, the carrier shall provide breakdowns for the following categories of cost elements, as applicable:

      (i) Materials.
      Provide a consolidated cost summary of individual material quantities included in the various tasks, orders, or agreement line items being proposed and the basis upon which they were developed (vendor quotes, invoice prices, etc.). Include raw materials, parts, software, components, and assemblies. For all items proposed, identify the item, source, quantity, and cost.

      (ii) Direct labor.
      Provide a time-phased (e.g., monthly, quarterly) breakdown of labor hours, rates, and costs by appropriate category, and furnish the methodologies used in developing estimates.

      (iii) Allocable direct costs.
      Indicate how allocable costs are computed and applied, including cost breakdowns that provide a basis for evaluating the reasonableness of proposed rates.

      (iv) Subcontracting costs.
      For any subcontractor costs submitted for reimbursement, the carrier is responsible for ensuring that documentation requirements set forth herein are
passed on to any and all subcontractors utilized in the carrier’s efforts to meet CALEA requirements.

(v) Other costs. List all other costs not otherwise included in the categories described above (e.g., special tooling, travel, computer and consultant services) and provide bases for costs.

(e) As part of the specific information required, the carrier shall submit with its cost estimate and clearly identify as such, costs that are verifiable and factual. In addition, the carrier shall submit information reasonably required to explain its estimating process, including:

1. The judgmental factors applied, such as trends or budgetary data, and the mathematical or other methods used in the estimate, including those used in projecting from known data; and

2. The nature and amount of any contingencies included in the proposed estimate.

(f) There is a clear distinction between submitting cost data and merely making available books, records, and other documents without identification. The requirement for submission of cost data is met when all accurate cost data reasonably available to the carrier have been submitted, either actually or by specific identification, to the FBI.

(g) In submitting its estimate, the carrier must include an index, appropriately referenced, of all the cost data and information accompanying or identified in the estimate. In addition, any future additions and/or revisions, up to the date of agreement on the costs, must be annotated in a supplemental index.

(h) Headings for submission are as follows:

1. Total Project Cost: Summary.
   
   (i) Cost Elements (Enter appropriate cost elements.)

   (ii) Proposed Cost Estimate—Total Cost (Enter those necessary and reasonable costs that in the carrier's judgment will properly be incurred in efficient completion of CALEA requirements. When any of the costs in this have already been incurred (e.g., under a letter contract), describe them on an attached supporting schedule.)

   (iii) Proposed Cost Estimate—Unit Cost (Enter the unit costs for each cost element.)
(iv) Supporting Material (Identify the attachment in which the information supporting the specific cost element may be found.)

(2) Total Project Costs: Detail (at Switch Level or Project Level, as appropriate).

(i) Cost Elements (Enter appropriate cost elements.)

(ii) Proposed Cost Estimate—Total Cost (Enter those necessary and reasonable costs that in the carrier's judgment will properly be incurred in efficient completion of CALEA requirements. When any of the costs in this have already been incurred (e.g., under a letter contract), describe them on an attached supporting schedule.)

(iii) Proposed Cost Estimate—Unit Cost (Enter the unit costs for each cost element.)

(iv) Supporting Material (Identify the attachment in which the information supporting the specific cost element may be found.)

28 CFR Section 100.17: Request for payment.

(a) The carrier shall provide sufficient supporting documentation at the time of submission of request for payment to allow adequate analysis and evaluation of the incurred costs. The FBI reserves the right to request additional cost data from carriers in order to ensure compliance with this part.

(b) Instructions for submission of the supporting documentation for the request for payment are as follows:

(1) The carrier shall submit to the FBI incurred costs by line item with supporting information.

(2) A cost element breakdown as described in § 100.17(f) shall be attached for each agreed upon line item.

(3) Supporting breakdowns shall be furnished for each cost element, consistent with the carrier's cost accounting system.

(c) When more than one line item has been agreed upon, summary total amounts covering all line items shall be furnished for each cost element. Depending on the carrier's accounting system, breakdowns shall be provided to the FBI for the following categories of cost elements, as applicable:
(1) Materials.

Provide a consolidated cost summary of individual material quantities included in the various tasks, orders, or agreement line items and the basis upon which they were determined (vendor invoices, time sheets, payroll records, etc.). Include raw materials, parts, software, components, and assemblies. For all reimbursable items, identify the item, source, quantity, and cost.

(2) Direct labor.

Provide a breakdown of labor hours, rates, and cost by appropriate category, and furnish the methodologies used in identifying these costs. Have available for audit, in accordance with § 100.18, time sheet and labor rate calculation justification for all direct labor charged to the agreement.

(3) Allocable direct costs.

Indicate how allocable costs are computed and applied, including cost breakdowns, comparing estimates to actual data as a basis for evaluating the reasonableness of actual costs.

(4) Subcontracting costs.

For any subcontractor costs submitted for reimbursement, along with a copy of the invoice, the carrier must have available for audit in accordance with § 100.18, documentation that costs incurred are just and reasonable.

(5) Other costs.

List all other costs not otherwise included in the categories described above (e.g., special tooling, travel, computer and consultant services) and have available for audit in accordance with § 100.18, documentation that costs incurred are just and reasonable.

(d) There is a clear distinction between submitting cost data and merely making available books, records, and other documents without identification.

(1) The requirement for submission of cost data is met when all accurate cost data reasonably available to the carrier have been submitted, either actually or by specific identification of the data that are available for review in the carrier's files, to the FBI.
(2) Should later information which affects the level of reimbursement come into the carrier's possession, it must be promptly submitted to the FBI.

(3) The requirement for submission of cost data continues up to the time of final reimbursement.

(e) In submitting its invoice, the carrier must include an index, which cross references the actual cost data submitted with the cost estimate.

(f) Headings for submission are as follows:

(1) Total Project Cost: Summary.

(i) Cost Elements (Enter appropriate cost elements.)

(ii) Actual Costs Incurred—Total Cost (Enter those necessary and reasonable costs that were incurred in the efficient completion of CALEA requirements.)

(iii) Actual Costs Incurred—Unit Cost (Enter the unit costs for each cost element.)

(iv) Supporting Material (Identify the attachment in which the information supporting the specific cost element may be found.)

(2) Total Project Costs: Detail (at Switch Level or Project Level, as appropriate.)

(i) Cost Elements (Enter appropriate cost elements.)

(ii) Actual Costs Incurred—Total Cost (Enter those necessary and reasonable costs that were incurred in the efficient completion of CALEA requirements.)

(iii) Actual Costs Incurred—Unit Cost (Enter the unit costs for each cost element.)

(iv) Supporting Material (Identify the attachment in which the information supporting the specific cost element may be found.)

28 CFR Section 100.18: Audit.

(a) General.
In order to evaluate the accuracy, completeness, and timeliness of the cost data, the FBI or other representatives of the Government shall have the right to examine and audit all of the carrier's supporting materials.

(1) These materials include, but are not limited to books, records, documents, and other data, regardless of form (e.g., machine readable media such as disk, tape) or type (e.g., data bases, applications software, data base management software, utilities), including computations and projections related to proposing, negotiating, costing, or performing CALEA compliance efforts or modifications.

(2) The right of examination shall extend to all documents necessary to permit adequate evaluation of the cost data submitted, along with the computations and projections used.

(b) Audits of request for payment.
The carrier shall maintain and the FBI or representatives of the Government shall have the right to examine and audit supporting materials.

(1) These materials include, but are not limited to, books, records, documents, and other evidence and accounting procedures and practices, regardless of form (e.g., machine readable media such as disk, tape) or type (e.g., data bases, applications software, data base management software, utilities), sufficient to reflect properly all costs claimed to have been incurred, or anticipated to be incurred, in performing the CALEA compliance effort.

(2) This right of examination shall include inspection at all reasonable times of the carrier's plants, or parts of them, engaged in performing the effort.

(c) Reports.
If the carrier is required to furnish cost, funding, or performance reports, the FBI or representatives of the Government shall have the right to examine and audit books, records, other documents, and supporting materials, for the purpose of evaluating the effectiveness of the carrier's policies and procedures to produce data compatible with the objectives of these reports and the data reported.

(d) Availability.
The carrier shall make available at its office at all reasonable times the costs and support material described herein, for examination, audit, or reproduction, until three (3) years after final reimbursement payment. In addition,

(1) If the CALEA compliance effort is completely or partially terminated, the records relating to the work terminated shall be made available for three (3) years after any resulting final termination settlement; and
(2) Records relating to appeals, litigation or the settlement of claims arising under or relating to the CALEA compliance effort shall be made available until such appeals, litigation, or claims are disposed of.

(e) Subcontractors.
The carrier shall ensure that all terms and conditions herein are incorporated in any agreement with a subcontractor that may be utilized by the carrier to perform any or all portions of the agreement.

28 CFR Section 100.19: Adjustments to agreement estimate.

(a) Adjustments prior to the incurrence of a cost.
   (1) In accordance with § 100.17(d)(2), the carrier shall notify the FBI when any change affecting the level of reimbursement occurs.

   (2) Upon such notification, if the adjustment results in an increase in the estimated reimbursement, the FBI will review the submission and determine if

       (i) Funds are available;

       (ii) The adjustment is justified and necessary to accomplish the goals of the agreement; and

       (iii) It is in the best interest of the government to approve the expenditure.

   (3) The FBI will provide the decision as to the acceptability of any increase to the carrier in writing.

(b) Adjustments after the incurrence of a cost.
   Any cost incurred that exceeds the provision in § 100.16(e)(2) will be reviewed by the FBI to determine reasonability, allowability, and if it is in the best interest of the government to approve the expenditure for reimbursement.

(c) Reduction for defective cost data.
   (1) The cost shall be reduced accordingly and the agreement shall be modified to reflect the reduction if any cost estimate negotiated in connection with the CALEA compliance effort, or any cost reimbursable under the effort is increased because:

       (i) The carrier or a subcontractor furnished cost data to the government that were not complete, accurate, and current;
(ii) A subcontractor or prospective subcontractor furnished the cost data to the carrier that were not complete, accurate, and current; or

(iii) Any of these parties furnished data of any description that were not accurate.

(2) Any reduction in the negotiated cost under §100.19(c)(1) due to defective data from a prospective subcontractor that was not subsequently awarded the subcontract shall be limited to the amount by which either the actual subcontract or the actual cost to the carrier, if there was no subcontract, was less than the prospective subcontract cost estimate submitted by the carrier, provided that the actual subcontract cost was not itself affected by defective cost data.

(3) If the FBI determines under §100.19(c)(1) that a cost reduction should be made, the carrier shall not raise the following matters as a defense:

(i) The carrier or subcontractor was a sole source supplier or otherwise was in a superior bargaining position and thus the costs of the agreement would not have been modified even if accurate, complete, and current cost data had been submitted;

(ii) The FBI should have known that the cost data at issue were defective even though the carrier or subcontractor took no affirmative action to bring the character of the data to the attention of the FBI;

(iii) The carrier or subcontractor did not submit accurate cost data. Except as prohibited, an offset in an amount determined appropriate by the FBI based upon the facts shall be allowed against the cost reimbursement of an agreement amount reduction if the carrier certifies to the FBI that, to the best of the carrier's knowledge and belief, the carrier is entitled to the offset in the amount requested and the carrier proves that the cost data were available before the date of agreement on the cost of the agreement (or cost of the modification) and that the data were not submitted before such date. An offset shall not be allowed if the understated data were known by the carrier to be understated when the agreement was signed; or the Government proves that the facts demonstrate that the agreement amount would not have increased even if the available data had been submitted before the date of agreement on cost; or

(4) In the event of an overpayment, the carrier shall be liable to and shall pay the United States at that time such overpayment as was made, with simple interest on the amount of such overpayment to be computed from the date(s) of overpayment to the carrier to the date the Government is repaid by the carrier at the applicable underpayment rate effective for each quarter prescribed by the Secretary of the Treasury under 26 U.S.C. 6621(a)(2).
28 CFR Section 100.20: Confidentiality of trade secrets/proprietary information.

With respect to any information provided to the FBI under this part that is identified as company proprietary information, it shall be treated as privileged and confidential and only shared within the government on a need-to-know basis. It shall not be disclosed outside the government for any reason inclusive of Freedom of Information requests, without the prior written approval of the company. Information provided will be used exclusively for the implementation of CALEA. This restriction does not limit the government's right to use the information provided if obtained from any other source without limitation.

28 CFR Section 100.21: Alternative dispute resolution.

(a) If an impasse arises in negotiations between the FBI and the carrier which precludes the execution of a cooperative agreement, the FBI will consider using mediation with the goal of achieving, in a timely fashion, a consensual resolution of all outstanding issues through facilitated negotiations.

(b) Should the carrier agree to mediation, the costs of that mediation process shall be shared equally by the FBI and the carrier.

(c) Each mediation shall be governed by a separate mediation agreement prepared by the FBI and the carrier.
28 CFR PART 105—CRIMINAL HISTORY BACKGROUND CHECKS

- Subpart A [Reserved]
- Subpart B—Aviation Training for Aliens and Other Designated Individuals
  - 28 CFR Section 105.10: Definitions, purpose, and scope.
  - 28 CFR Section 105.11: Individuals not requiring a security risk assessment.
  - 28 CFR Section 105.12: Notification for candidates eligible for expedited processing.
  - 28 CFR Section 105.13: Notification for candidates not eligible for expedited processing.
- Subpart C—Private Security Officer Employment
  - 28 CFR Section 105.21: Purpose and authority.
  - 28 CFR Section 105.23: Procedure for requesting criminal history record check.
  - 28 CFR Section 105.24: Employee’s rights.
  - 28 CFR Section 105.25: Authorized employer’s responsibilities.
  - 28 CFR Section 105.26: State agency’s responsibilities.
  - 28 CFR Section 105.27: Miscellaneous provisions.

Authority:

Source:
Order No. 2656-2003, 68 FR 7318, February 13, 2003, unless otherwise noted.
SUBPART A [Reserved]

SUBPART B—Aviation Training for Aliens and Other Designated Individuals

28 CFR Section 105.10: Definitions, purpose, and scope.

(a) Definitions.

ATSA

means the Aviation and Transportation Security Act, Public Law 107-71.

Candidate

means any person who is an alien as defined in section 101(a)(3) of the Immigration and Nationality Act, 8 U.S.C. 1101(a)(3), or a person specified by the Under Secretary of Transportation for Security, who seeks training in the operation of an aircraft with a maximum certificated takeoff weight of 12,500 pounds or more from a Provider.

Certificates with ratings recognized by the United States

means a valid pilot or flight engineer certificate with ratings issued by the United States, or a valid foreign pilot or flight engineer license issued by a member of the Assembly of the International Civil Aviation Organization, as established by Article 43 of the Convention on International Civil Aviation.

Notification

means providing the information required under this regulation in the format and manner specified.

Provider

means a person or entity subject to regulation under Title 49 Subtitle VII, Part A, United States Code. This definition includes individual training providers, training centers, certificated carriers, and flight schools. Virtually all private
providers of instruction in the operation of aircraft with a maximum certificated takeoff weight of 12,500 pounds or more are covered by section 113 of ATSA (49 U.S.C. 44939) and are therefore subject to this rule. Providers located in countries other than the United States are included in this definition to the extent that they are providing training leading to a United States license, certification, or rating. Providers who “dry-lease” simulator equipment to individuals or entities for use within the United States are deemed to be providing the training themselves if the lessee is not subject to regulation under Title 49. Providers located in countries other than the United States who are providing training that does not lead to a United States pilot or flight engineer certification, or rating are not included in this definition. When the Department of Defense or the U.S. Coast Guard, or an entity providing training pursuant to a contract with the Department of Defense or the U.S. Coast Guard (including a subcontractor), provides training for a military purpose, such training is not subject to Federal Aviation Administration (FAA) regulation. Accordingly, these entities, when providing such training, are not “person[s] subject to regulation under this part” within the meaning of section 113 of ATSA.

Training

means any instruction in the operation of an aircraft, including “ground school,” flight simulator, and in-flight training. It does not include the provision of training manuals or other materials, and does not include mechanical training that would not enable the trainee to operate the aircraft in flight.

(b) Purpose and scope.

(1) Section 113 of ATSA (49 U.S.C. 44939) prohibits Providers from furnishing candidates with training in the operation of an aircraft with a maximum certificated takeoff weight of 12,500 pounds or more without the prior notification of the Attorney General. Training in the operation of smaller aircraft is considered to be training in the operation of an aircraft with a maximum certificated takeoff weight of 12,500 pounds or more if the training would lead to a type rating allowing the candidate to operate a model of the same or substantially similar type of aircraft with a maximum certificated takeoff weight of 12,500 pounds or more in accordance with FAA regulations. The purpose of this notification is to allow the Attorney General to determine whether such an individual presents a risk to aviation or national security before training may begin. The Department believes that it is not required to make a candidate wait for 45 days in order to begin training if the Department has completed its risk assessment. Therefore, after providing the required notification to the Attorney General as described in this subpart, the Provider may begin instruction of a candidate if the Attorney General has informed the Provider that the Attorney General has determined as a result of the risk assessment conducted pursuant to section 113 of ATSA that providing the training does not present a risk to aviation
or national security. If the Attorney General does not provide either an authorization to proceed with training or a notice to deny training within 45 days after receiving the required notification, the Provider may commence training at that time. All candidates who are not citizens or nationals of the U.S. must show a valid passport establishing their identity to a Provider before commencing training.

(2) The Department may, at any time, require the resubmission of all or a portion of a candidate’s training request, including fingerprints. If, after approving any training application, the Department determines that a candidate presents a risk to aviation or national security, it will notify the Provider to cease training. The Provider who submitted the candidate’s identifying information will be responsible for ensuring that the training is promptly halted, regardless of whether another Provider is currently training the candidate.

(3) Providing false information or otherwise failing to comply with section 113 of ATSA may present a threat to aviation or national security and is subject to both civil and criminal sanctions. The United States will take all necessary legal action to deter and punish violations of this section.

(4) Providers should make every effort to ensure that approved training occurs on the dates specified in the training request at the location of the Provider who submitted the request. However, where scheduling problems or other exigent circumstances prevent this from happening, training may be rescheduled for any time within 30 days of the approved training dates without submitting an additional request. If any scheduling change of greater than 30 days occurs, a new request with the corrected training dates must be submitted. Any proposed change in location or Provider must precipitate a new request, although Providers may employ the assistance of other Providers or their facilities for a portion of the training, provided that the substantial majority of the training occurs at location of the Provider who submitted the request.

28 CFR Section 105.11: Individuals not requiring a security risk assessment.

(a) Citizens and nationals of the United States.
A citizen or national of the United States is not subject to section 113 of ATSA unless otherwise designated by the Under Secretary of Transportation for Security. A Provider must determine whether a prospective trainee is a citizen or national of the United States prior to providing training in the operation of an aircraft with a maximum certificated takeoff weight of 12,500 pounds or more. To establish United States citizenship or nationality, the prospective trainee must
show the Provider from whom he or she seeks training any of the following documents as proof of United States citizenship or nationality:

(1) A valid, unexpired United States passport;

(2) An original or government-issued certified birth certificate with a registrar's raised, embossed, impressed or multicolored seal, registrar's signature, and the date the certificate was filed with the registrar's office, which must be within 1 year of birth, together with a government-issued picture identification of the individual named in the birth certificate (the birth certificate must establish that the person was born in the United States or in an outlying possession, as defined in section 101(a)(29) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(29));

(3) An original United States naturalization certificate with raised seal, INS Form N-550 or INS Form N-570, together with a government-issued picture identification of the individual named in the certificate;

(4) An original certification of birth abroad with raised seal, Department of State Form FS-545 or Form DS-1350, together with a government-issued picture identification of the individual named in the certificate;

(5) An original certificate of United States citizenship with raised seal, INS Form N-560 or Form N-561, together with a government-issued picture identification of the individual named in the certificate; or

(6) In the case of training provided to a federal employee (including military personnel) pursuant to a contract between a federal agency and a Provider, the agency's written certification as to its employee's United States citizenship/nationality, together with the employee’s government-issued credentials or other federally-issued picture identification.

(b) Exception.
Notwithstanding paragraph (a) of this section, a Provider is required to provide notification to the Attorney General with respect to any individual specified by the Under Secretary of Transportation for Security. Individuals specified by the Under Secretary of Transportation for Security will be identified by procedures developed by the Department of Transportation and are not eligible for expedited processing under § 105.12 of this part.

28 CFR Section 105.12: Notification for candidates eligible for expedited processing.

(a) Expedited processing.
The Attorney General has determined that providing aviation training to certain categories of candidates presents a minimal additional risk to aviation or national security because of the aviation training already possessed by these individuals or because of risk assessments conducted by other agencies. Therefore, the following categories of candidates are eligible for expedited processing, unless the candidate is an individual specified by the Under Secretary of Transportation for Security:

(1) Foreign nationals who are current and qualified as pilot in command, second in command, or flight engineer with respective certificates with ratings recognized by the FAA for aircraft with a maximum certificated takeoff weight of over 12,500 pounds, or who are currently employed and qualified by U.S. regulated air carriers as pilots on aircraft with a maximum certificated takeoff weight of 12,500 pounds or more;

(2) Foreign nationals who are commercial, governmental, corporate, or military pilots of aircraft with a maximum certificated takeoff weight of 12,500 pounds or more who are receiving training on a particular aircraft in connection with the sale of that aircraft, provided that the training provided is limited to familiarization (i.e., training required by one who is already a competent pilot to become proficient in configurations and variations of a new aircraft) and not initial qualification or type rating; or

(3) Foreign military or law enforcement personnel who must receive training on a particular aircraft given by the United States to a foreign government pursuant to a draw-down authorized by the President under section 506(a)(2) of the Foreign Assistance Act of 1961, as amended (22 U.S.C. 2318(a)(2)), if the training provided is limited to familiarization.

(b) Notification.
Before a Provider may conduct training for a candidate eligible for expedited processing under paragraph (a) of this section, the Provider must submit the following information to the Department:

(1) The full name of the candidate;

(2) A unique student identification number created by the Provider as a means of identifying records concerning the candidate;

(3) Date of birth;

(4) Country of citizenship;

(5) Passport issuing authority;
(6) Dates of training; and

(7) The category of expedited processing under paragraph (a) of this section for which the candidate qualifies.

(c) Commencement of training.

(1) The notification must be provided electronically to the Department by the Provider in the specific format and by the specific means identified by the Department. Notification must be made by electronic mail. Only notifications sent from an electronic mail address registered as a Provider will be accepted. Specific details about the mechanism for the notification will be made available by the Department and distributed through the FAA.

(2) After the complete notification is furnished to the Department, the Provider may commence training the candidate as soon as the Provider receives a response from the Department that the individual does not present a risk to aviation or national security as a result of the risk assessment conducted pursuant to section 113 of ATSA and the foreign national candidate presents a valid passport establishing his or her identity to the Provider. Receipt of this response from the Department will be deemed approval by the Department to commence training.

(d) Records.

When a Provider conducts training for a candidate eligible for expedited processing, the Provider must retain a copy of the relevant pages of the passport and other records to document how the Provider made the determination that the candidate was eligible. The Provider also must retain certain identifying records regarding the candidate, including date of birth, place of birth, passport issuing authority, and passport number. The Provider must be able to reference these records by the unique student identification number provided to the Department pursuant to this section. Providers also are encouraged to maintain photographs of all candidates trained by the Provider. Such records must be maintained for at least three years following the conclusion of training by the Provider. The Provider must also be able to use the unique student identification number to cross-reference any other documentation that the FAA may require the Provider to retain regarding the candidate.

28 CFR Section 105.13: Notification for candidates not eligible for expedited processing.

(a) A Provider must submit a complete Flight Training Candidate Checks Program (FTCCP) form and arrange for the submission of fingerprints to the Department in accordance with this section prior to providing flight training,
except with respect to persons whom the Provider has determined, as provided in § 105.11 of this part, are not subject to a security risk assessment. A separate FTCCP form must be submitted for each course or instance of training requested by a candidate. A set of fingerprints must be submitted in accordance with this rule prior to the commencement of any training. Where a Provider enlists the assistance of another Provider in training a candidate, no additional request need be submitted, as long as the specific instance of training has been approved.

(b) The completed FTCCP form must be sent to the Attorney General via electronic submission at https://www.flightschoolcandidates.gov. The form must be submitted no more than three months prior to the proposed training dates. No paper submissions of this form will be accepted.

(1) In order to ensure that such electronic submissions are made by FAA certificated training providers, Providers must receive initial access to the system through the FAA. Providers should register through their local FAA Flight Standards District Offices. The FAA has decided that registration will be only by appointment. Upon registration, Providers will be sent (via electronic mail) an access password to use the system.

(2) Candidates may complete the online FTCCP form at https://www.flightschoolcandidates.gov to reduce the burden on the Provider. After the form has been completed by a candidate, it will be forwarded electronically to the Provider for verification that the candidate is a bona fide applicant. Verification by the Provider will be considered submission of the form for purposes of paragraph (a) of this section. To reduce the burden on the candidates, personal information needs only to be updated, rather than reentered, for each subsequent training request.

(c) Candidates must submit fingerprints to the Federal Bureau of Investigation (FBI) as part of the identification process. These fingerprints must be taken by, or under the supervision of, a federal, state, or local law enforcement agency, or by another entity approved by the Director of the Foreign Terrorist Tracking Task Force, in consultation with the FBI’s Criminal Justice Information Services Division. Where available, fingerprints may be taken by U.S. government personnel at a United States embassy or consulate. Law enforcement agencies and U.S. diplomatic installations are not required to participate in this process, but their cooperation is strongly encouraged. Any individual taking fingerprints as part of the notification process must comply with the following requirements when taking and processing fingerprints to ensure the integrity of the process:

(1) Candidates must provide two forms of identification at the time of fingerprinting. In the case of aliens, one of the forms of identification must be the individual’s passport. In the case of United States citizens or nationals designated
by the Under Secretary of Transportation for Security, a valid photo driver's license issued in the United States may be submitted in lieu of a passport;

(2) The fingerprints must be taken under the direct observation of a law enforcement or consular officer, or another specifically authorized individual. Individuals other than law enforcement or consular officers will only be approved on a case-by-case basis by the Director of the Foreign Terrorist Tracking Task Force, in consultation with the FBI's Criminal Justice Information Services Division, upon a showing that they possess the necessary training and will ensure the integrity of the fingerprinting process;

(3) The fingerprints must be processed by means approved by the Director of the Foreign Terrorist Tracking Task Force, in consultation with the FBI's Criminal Justice Information Services Division;

(4) The fingerprint submissions must be forwarded to the FBI in the manner specified by the Director of the Foreign Terrorist Tracking Task Force, in consultation with the FBI's Criminal Justice Information Services Division;

(5) Officials taking fingerprints must ensure that any fingerprints provided to the FBI are not placed within the control of the candidate or the Provider at any time; and

(6) Candidates must pay for all costs associated with taking and processing their fingerprints.

(d) In accordance with Public Law 101-515, as amended, the Director of the FBI is authorized to establish and collect fees to process fingerprint identification records and name checks for certain purposes, including non-criminal justice and licensing purposes. In addition to the cost to the FBI for conducting its review, other fees may be imposed, including the cost of taking the fingerprints and the cost of processing the fingerprints and submitting them to the FBI for review. Because the total fee may vary by agency, the candidate must check with the entity taking the fingerprints to determine the applicable total fee. This payment must be made at the designated rate for each set of fingerprints submitted.

(e) In some cases, candidates seeking training from Providers abroad may be unable to obtain fingerprints. If a Provider located in a country other than the United States can demonstrate that compliance with the fingerprint requirement is not practicable, a temporary waiver of the requirement may be requested by contacting the Foreign Terrorist Tracking Task Force. The Director of the Foreign Terrorist Tracking Task Force will have the discretion to grant the waiver, deny the waiver, or prescribe a reasonable, alternative manner of complying with the fingerprint requirement for each Provider location.
(f) The 45-day review period by the Department will not start until all the required information has been submitted, including fingerprints.

28 CFR Section 105.14: Risk assessment for candidates.

(a) It is the responsibility of the Department of Justice to conduct a risk assessment for each candidate. The Department has made an initial determination that providing training to the aliens in the categories set forth in § 105.12(a) of this part presents minimal additional risk to aviation or national security and therefore has established an expedited processing procedure for these aliens. Based on the information contained in each FTCCP form and the corresponding set of fingerprints, the Department will determine whether a candidate not granted expedited processing presents a risk to aviation or national security.

(b) After submission of the FTCCP form by the Provider, the Department will perform a preliminary risk assessment.

(1) If the Department determines that a candidate does not present a risk to aviation or national security as a result of the preliminary risk assessment, the candidate or the Provider will be notified electronically that the Provider may supply the candidate with the appropriate materials and instructions to complete the fingerprinting process described in § 105.13(c) and (d) of this part.

(2) If the Department determines that the candidate presents a risk to aviation or national security, when appropriate, it will notify the Provider electronically that training is prohibited.

(3) For each complete training request submitted by a Provider, the Department will promptly conduct an appropriate risk assessment. Every effort will be made to respond to a training request in the briefest time possible. In routine cases, the Department anticipates granting approval to train within a fraction of the 45-day notification period after receiving a complete, properly submitted request, including fingerprints. In the unlikely event that no notification or authorization by the Department has occurred within 45 days after the proper submission under these regulations of all the required information, the Provider may proceed with the training, upon establishing the candidate's identity in accordance with paragraph (c) of this section.

(c) Providers must ascertain the identity of each candidate. For candidates who are not citizens or nationals of the United States designated by the Under Secretary of Transportation for Security, a Provider must inspect the candidate’s passport and visa to verify the candidate’s identity before providing training. Candidates who are citizens or nationals of the United States must present the
documentation described in § 105.11(a) of this part. If the candidate's identity cannot be verified, then the Provider cannot proceed with training.

(d) If, at any time after training has begun, the Department determines that a candidate subject to this section being trained by a Provider presents a risk to aviation or national security, the Department shall notify the Provider to cease training. A Provider so notified shall immediately cease providing any training to the person, regardless of whether or in what manner such training commenced or had been authorized. The Provider who submitted the candidate's identifying information will be responsible for ensuring that the training is promptly halted, regardless of whether another Provider is currently training the candidate.

(e) With regard to any determination as to an alien candidate's eligibility for training, when appropriate, the Department will inform the Secretary of State and the Secretary of Homeland Security as to the identity of the alien and the determination made.
SUBPART C—Private Security Officer Employment

Authority:

Source:
Order No. 2796-2006, 71 FR 1693, Jan. 11, 2006, unless otherwise noted.

28 CFR Section 105.21: Purpose and authority.
(a) The purpose of this subpart is to regulate the exchange of criminal history record information (“CHRI”), as defined in 28 CFR 20.3(d), and related information authorized by Section 6402 (The Private Security Officer Employment Authorization Act of 2004) (Act) of Public Law 108-458 (The Intelligence Reform and Terrorism Prevention Act of 2004). Section 6402 authorizes a fingerprint-based criminal history check of state and national criminal history records to screen prospective and current private security officers, and section 6402(d)(2) requires the Attorney General to publish regulations to provide for the “security, confidentiality, accuracy, use, submission, dissemination, destruction of information and audits, and record keeping” of the CHRI and related information, standards for qualifying an authorized employer, and the imposition of fees.

(b) The regulations in this subpart do not displace state licensing requirements for private security officers. A State retains the right to impose its own licensing requirements upon this industry.

28 CFR Section 105.22: Definitions.
As used in this subpart:

(a) Authorized employer
means any person that employs private security officers and is authorized by the regulations in this subpart to request a criminal history record information search of an employee through a state identification bureau. An employer is not authorized within the meaning of these regulations if it has not executed and submitted to the appropriate state agency the certification required in § 105.25(g), if its authority to do business in a State has been suspended or revoked pursuant to state law, or, in those states that regulate private security officers, the employer has been found to be out of compliance with any mandatory standards or requirements established by the appropriate regulatory agency or entity.

(b) Employee
means both a current employee and an applicant for employment as a private security officer.

(c) Charged, with respect to a criminal felony, means being subject to a complaint, indictment, or information.

(d) Felony means a crime punishable by imprisonment for more than one year, regardless of the period of imprisonment actually imposed.

(e) Participating State means a State that has not elected to opt out of participating in the Act by statutory enactment or gubernatorial order. A State may decline to participate in the background check system authorized by the Act by enacting a law or issuing an order by the Governor (if consistent with state law) providing that the State is declining to participate. The regulations in this subpart that pertain to States apply only to participating states.

(f) Person means an individual, partnership, firm, company, corporation or institution that performs security services, whether for a third party for consideration or as an internal, proprietary function.

(g) Private Security Officer means an individual other than an employee of a Federal, State, or local government whose primary duty is to perform security services, full or part time, for consideration, whether armed or unarmed and in uniform or plain clothes, except as may be excluded from coverage in these regulations, except that the term excludes—

1. Employees whose duties are primarily internal audit or credit functions;

2. Employees of electronic security system companies acting as technicians or monitors; or

3. Employees whose duties involve the secure movement of prisoners.

(h) Security services means services, whether provided by a third party for consideration, or by employees as an internal, proprietary function, to protect people or property, including activities to: Patrol, guard, or monitor property (including real property as well as tangible or intangible personal property such as records, merchandise, money, and equipment); protect against fire, theft, misappropriation, vandalism, violence, terrorism, and other illegal activity; safeguard persons; control access to
real property and prevent trespass; or deter criminal activity on the authorized
employer's or another's premises. This definition does not cover services by the
employees described in § 105.22(f) as excluded from the definition of private
security officer.

(i) State Identification Bureau (SIB)
means the state agency designated by the Governor or other appropriate
executive official or the state legislature to perform centralized recordkeeping
functions for criminal history records and associated services in the States.

28 CFR Section 105.23: Procedure for requesting criminal history
record check.

These procedures only apply to participating states. An authorized employer may
obtain a State and national criminal history record check as authorized by section
6402 of Public Law 105-458 as follows:

(a) An authorized employer is required to execute a certification to the State,
developed by the SIB or the relevant state agency for purposes of accepting
requests for these background checks, declaring that it is an authorized employer
that employs private security officers; that all fingerprints and requests for
criminal history background checks are being submitted for private security
officers; that it will use the information obtained as a result of the state and
national criminal history record checks solely for the purpose of screening its
private security officers; and that it will abide by other regulatory obligations. To
help ensure that only legitimate use is made of this authority, the certification
shall be executed under penalties of perjury, false statement, or other applicable
state laws.

(b) An authorized employer must obtain a set of fingerprints and the written
consent of its employee to submit those prints for a state and national criminal
history record check. An authorized employer must submit the fingerprints and
appropriate state and federal fees to the SIB in the manner specified by the SIB.

(c) Upon receipt of an employee's fingerprints, the SIB shall perform a
fingerprint-based search of its criminal records. If no relevant criminal record is
found, the SIB shall submit the fingerprints to the FBI for a national search.

(d) Upon the conclusion of the national search, the FBI will disseminate the
results to the SIB.

(e) Based upon the results of the state check and, if necessary, the national check:
(1) If the State has standards for qualifying a private security officer, the SIB or other designated state agency shall apply those standards to the CHRI and notify the authorized employer of the results of the application of the state standards; or

(2) If the State does not have standards for qualifying a private security officer, the SIB or other designated state agency shall notify an authorized employer as to the fact of whether an applicant has been:

   (i) Convicted of a felony;

   (ii) Convicted of a lesser offense involving dishonesty or false statement if occurring within the previous ten years;

   (iii) Convicted of a lesser offense involving the use or attempted use of physical force against the person of another if occurring within the previous ten years; or

   (iv) Charged with a felony during the previous 365 days for which there has been no resolution.

(f) The limitation periods set forth in paragraph (e)(2) of this section shall be determined using the date the employee’s fingerprints were submitted. An employee shall be considered charged with a criminal felony for which there has been no resolution during the preceding 365 days if the individual is the subject of a complaint, indictment, or information, issued within 365 days of the date that the fingerprints were taken, for a crime punishable by imprisonment for more than one year. The effect of various forms of post-conviction relief shall be determined by the law of the convicting jurisdiction.

28 CFR Section 105.24: Employee’s rights.

An employee is entitled to:

(a) Obtain a copy from the authorized employer of any information concerning the employee provided under these regulations to the authorized employer by the participating State;

(b) Determine the status of his or her CHRI by contacting the SIB or other state agency providing information to the authorized employer; and

(c) Challenge the CHRI by contacting the agency originating the record or complying with the procedures contained in 28 CFR 16.34.
An authorized employer is responsible for:

(a) Executing and providing to the appropriate state agency the certification to the State required under § 105.23(a) before a State can accept requests on private security guard employees;

(b) Obtaining the written consent of an employee to submit the employee's fingerprints for purposes of a CHRI check as described herein;

(c) Submitting an employee's fingerprints and appropriate state and federal fees to the SIB not later than one year after the date the employee's consent is obtained;

(d) Retaining an employee's written consent to submit his fingerprints for a criminal history record check for a period of no less than three years from the date the consent was last used to request a CHRI check;

(e) Upon request, providing an employee with confidential access to and a copy of the information provided to the employer by the SIB; and

(f) Maintaining the confidentiality and security of the information contained in a participating State's notification by:

   (1) Storing the information in a secure container located in a limited access office or space;

   (2) Limiting access to the information strictly to personnel involved in the employer's personnel and administration functions; and

   (3) Establishing internal rules on the handling and dissemination of such information and training personnel with such access on such rules, on the need to safeguard and control the information, and on the consequences of failing to abide by such rules.

(a) Each State will determine whether it will opt out of participation by statutory enactment or gubernatorial order and communicating such determination to the
Attorney General. Failure to inform the Attorney General of the determination will result in a State being considered a participating State.

(b) Each participating State is responsible for:

(1) Determining whether to establish a fee to perform a check of state criminal history records and related fees for administering the Act;

(2) Developing a certification form for execution by authorized employers under § 105.25(a) and receiving authorized employers' certifications;

(3) Receiving the fingerprint submissions and fees from the authorized employer; performing a check of state criminal history records; if necessary, transmitting the fingerprints to the FBI; remitting the FBI fees consistent with established interagency agreements; and receiving the results of the FBI check;

(4) Applying the relevant standards to any CHRI returned by the fingerprint check and notifying the authorized employer of the results of the application of the standards as required under § 105.23(e);

(5) Providing to an employee upon his or her request a copy of CHRI upon which an adverse determination was predicated; and

(6) Maintaining, for a period of no less than three years, auditable records regarding

   (i) Maintenance and dissemination of CHRI; and

   (ii) The employer's certification.

(c) If relevant CHRI is lacking disposition information, the SIB or responsible agency in a participating State will make reasonable efforts to obtain such information to promote the accuracy of the record and the integrity of the application of the relevant standards. If additional time beyond a State's standard response time is needed to find relevant disposition information, the SIB or responsible agency may advise the authorized employer that additional research is necessary before a final response can be provided. If raised, a participating State should take into account the effect of post-conviction relief.

28 CFR Section 105.27: Miscellaneous provisions.

(a) Alternate State availability.
(1) An authorized employer may submit the employee’s fingerprints to the SIB of a participating State other than the State of employment—provided it obtains the permission of the accommodating State—if the authorized employer is prevented from submitting an employee’s fingerprints because the employee’s employment is in:

(i) A State that does not have an applicable Public Law 92-544 statute authorizing state and national fingerprint-based criminal history checks of prospective and current private security officers and has elected to opt out; or

(ii) A participating State that has not yet established a process for receiving fingerprints and processing the checks under the regulations in this subpart.

(2) A participating State agreeing to process checks under this subsection will discontinue doing so if thereafter the State of the employee’s employment establishes a process State and national fingerprint-based criminal history checks of prospective and current private security officers.

(b) FBI fees for national check.

The fee imposed by the FBI to perform a fingerprint-based criminal history record check is that routinely charged for noncriminal justice fingerprint submissions as periodically noticed in the Federal Register.

(c) Penalties for misuse.

(1) In addition to incarceration for a period not to exceed two years, one who knowingly and intentionally misuses information (including a State’s notification) received pursuant to the Act may be subject to a fine pursuant to 18 U.S.C. 3571.

(2) Consistent with State law, a violation of these regulations may also result in the divestiture of “authorized employer” status, thereby precluding an employer which provides security services from submitting fingerprints for a State and national criminal history record check.

(d) Exclusion from coverage.

[Reserved]
28 CFR PART 200—ALIEN TERRORIST REMOVAL PROCEDURES

Authority:

Source:

28 CFR Section 200.1: Eligibility for Protection under the Convention Against Torture.

A removal order under Title V of the Act shall not be executed in circumstances that would violate Article 3 of the United Nations Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, subject to any reservations, understandings, declarations, and provisos contained in the United States Senate resolution of ratification of the Convention, as implemented by section 2242 of the Foreign Affairs Reform and Restructuring Act of 1998, Pub. L. 105-277. Convention-based claims by aliens subject to removal under this Title shall be determined by the Attorney General, in consultation with the Secretary of State.
Procedures for disclosure of records pursuant to the Freedom of Information Act
Administration of records under the Privacy Act of 1974
Procedures governing the acceptance of service of process
Production of ODNI information or material in proceedings before Federal, State, local or other government entity of competent jurisdiction
32 CFR PART 1700—PROCEDURES FOR DISCLOSURE OF RECORDS PURSUANT TO THE FREEDOM OF INFORMATION ACT

Current and revised as of July 1, 2011

- 1700.1: Authority and purpose.
- 1700.2: Definitions.
- 1700.3: Contact for general information and requests.
- 1700.4: Preliminary information.
- 1700.5: Requirements as to form and content.
- 1700.6: Fees for records services.
- 1700.7: Processing of requests for records.
- 1700.8: Action on the request.
- 1700.9: Payment of fees, notification of decision, and right of appeal.
- 1700.10: Procedures for business information.
- 1700.11: Procedures for information concerning other persons.
- 1700.12: Requests for expedited processing.
- 1700.13: Right to appeal and appeal procedures.
- 1700.14: Action by appeals authority.

Authority:

Source:
72 FR 45894, Aug. 16, 2007, unless otherwise noted.
32 CFR Section 1700.1: Authority and purpose.

(a) Authority.


(b) Purpose in general.

This part prescribes procedures for:
(1) ODNI administration of the FOIA;
(2) Requesting records pursuant to the FOIA; and
(3) Filing an administrative appeal of an initial adverse decision under the FOIA.

32 CFR Section 1700.2: Definitions.

For purposes of this Part, the following terms have the meanings indicated:

(a) Days

means calendar days when ODNI is operating and specifically excludes Saturdays, Sundays, and legal public holidays;

(b) Direct costs

means those expenditures which ODNI actually incurs in the processing of a FOIA request; it does not include overhead factors such as space;

(c) Pages

means paper copies of standard office size or the dollar value equivalent in other media;

(d) Reproduction

means generation of a copy of a requested record in a form appropriate for release;

(e) Review

means all time expended in examining a record to determine whether any portion must be withheld pursuant to law and in effecting any required deletions but excludes personnel hours expended in resolving general legal or policy issues; it also means personnel hours of professional time;
(f) Search

means all time expended in looking for and retrieving material that may be responsive to a request utilizing available paper and electronic indices and finding aids; it also means personnel hours of professional time or the dollar value equivalent in computer searches;

(g) Expression of interest

means a written or electronic communication submitted by any person requesting information on or concerning the FOIA program, the availability of documents from ODNI, or both;

(h) Fees

means those direct costs which may be assessed a requester considering the categories established by the FOIA; requesters should submit information to assist the ODNI in determining the proper fee category and the ODNI may draw reasonable inferences from the identity and activities of the requester in making such determinations; the fee categories include:

(1) Commercial use request:
A request in which the disclosure sought is primarily in the commercial interest of the requester and which furthers such commercial, trade, income or profit interests;

(2) Educational institution:
A preschool, a public or private elementary or secondary school, an institution of undergraduate higher education, an institution of graduate higher education, an institution of professional education, or an institution of vocational education, that operates a program of scholarly research. To be in this category, a requester must show that the request is authorized by and is made under the auspices of a qualifying institution and that the records are not sought for a commercial use but are sought to further scholarly research.

(3) Noncommercial scientific institution:
An institution that is not operated on a commercial basis, as that term is defined in paragraph (h)(1) of this section, and that is operated solely for the purpose of conducting scientific research the results of which are not intended to promote any particular product or industry. To be in this category, a requester must show that the request is authorized by and is made under the auspices of a qualifying institution and that the records are not sought for a commercial use but are sought to further scientific research.

(4) Representative of the news media:
An individual actively gathering news for an entity that is organized and operated to publish and broadcast news to the public and pursuant to the entity’s news dissemination function and not its commercial interests; the term “news” means
information which concerns current events, would be of current interest to the
general public, would enhance the public understanding of the operations or
activities of the U.S. Government, and is in fact disseminated to a significant
element of the public at minimal cost; freelance journalists are included in this
definition if they provide sufficient evidence to justify an expectation of
publication through such an organization, even though not actually employed by
it; a publication contract or prior publication record is relevant to such status;

(5) All other:
A request from an individual not within paragraphs (h)(1), (2), (3), or (4) of this
section;

(i) Freedom of Information Act, “FOIA,” or “the Act”

means the statute as codified at 5 U.S.C. 552;

(j) ODNI

means the Office of the Director of National Intelligence and its component
organizations. It does not include other members of the Intelligence Community
as defined in 50 U.S.C. 401a, or other federal entities subsequently designated in
accordance with this authority, unless specifically designated as included in this
part or in the notice of a system of records;

(k) Potential requester

means a person, organization, or other entity who submits an expression of
interest.

32 CFR Section 1700.3: Contact for general information and
requests.
For general information on this Part, to inquire about the FOIA program at
ODNI, or to file a FOIA request (or expression of interest), please direct
communication in writing to the Office of the Director of National Intelligence,
Chief FOIA Officer c/o Director, Information Management Office, Washington,
DC 20511 by mail or by facsimile at (703) 482-2144. FOIA requests can also be
submitted by electronic mail to FOIA @ dni.gov.

For general information or status information on pending cases only, call the
ODNI FOIA Customer Service Center at (571) 204-4774.

32 CFR Section 1700.4: Preliminary information.
Members of the public shall address all communications to the point of contact
specified in § 1700.3 and clearly delineate the communication as a request under
the FOIA. ODNI staff who receive a FOIA request shall expeditiously forward the
request to the Director, Information Management Office (IMO). Requests and
appeals (as well as referrals and consultations) received from FOIA requesters

____________________________________________________________

Page 875
who owe outstanding fees for information services at this or other federal agencies will not be accepted and action on all pending requests shall be terminated in such circumstances.

32 CFR Section 1700.5: Requirements as to form and content.

(a) Required information.

No particular form is required. A request must reasonably describe the record or records being sought and be submitted in accordance with this regulation. Documents must be described sufficiently to enable a staff member familiar with the subject to locate the documents with a reasonable amount of effort. Whenever possible, your request should include specific information about each record sought, such as the date, title or name, author, recipient, and the subject matter of the record. As a general rule, the more specific you are about the records or type of records that you want, the more likely it will be that the IMO will be able to locate records responsive to your request. The IMO will provide you an opportunity to discuss your request with it so that you may modify your request to meet the requirements of this section. If after having been asked to do so you do not provide the IMO with information sufficient to enable it to locate responsive records your request will be closed.

(b) Additional information for fee determination

A requester must provide sufficient personally identifying information to allow staff to determine the appropriate fee category and to contact the requester easily.

32 CFR Section 1700.6: Fees for records services.

(a) In general.

Search, review, and reproduction fees will be charged in accordance with the provisions below relating to schedule, limitations, and category of requester. Applicable fees will be due even if a subsequent search locates no responsive records or some or all of the responsive records must be denied under one or more of the exemptions of the FOIA.

(b) Fee waiver requests.

Records will be furnished without charge or at a reduced rate when ODNI determines:

(1) As a matter of administrative discretion, the interest of the United States Government would be served, or
(2) It is in the public interest to provide responsive records because the disclosure is likely to contribute significantly to the public understanding
of the operations or activities of the United States Government and is not primarily in the commercial interest of the requester.

(c) Fee waiver appeals.

Denials of requests for fee waivers or reductions may be appealed to the Director of the Intelligence Staff, or his functional equivalent, through the ODNI Chief FOIA Officer. A requester is encouraged to provide any explanation or argument as to how his or her request satisfies the requirements of this regulation and the Act. See § 1700.14 for further details on appeals.

(d) Time for fee waiver requests and appeals.

Appeals should be resolved prior to the initiation of processing and the incurring of costs. However, fee waiver requests will be accepted at any time prior to an agency decision regarding the request, except when processing has been initiated, in which case the requester must agree to be responsible for costs in the event of an adverse administrative or judicial decision.

(e) Agreement to pay fees.

If you make a FOIA request, it shall be considered a firm commitment by you to pay all applicable fees chargeable under this regulation, up to and including the amount of $25.00, unless you ask for a waiver of fees. When making a request, you may specify a willingness to pay a greater or lesser amount.

(f) Advance payment.

The ODNI may require an advance payment of up to 100 percent of the estimated fees when projected fees exceed $250.00, not including charges associated with the first 100 pages of production and two hours of search (when applicable), or when the requester previously failed to pay fees in a timely fashion, for fees of any amount. ODNI will hold in abeyance for 45 days those requests where advance payment has been requested.

(g) Schedule of fees [Incomplete]

(1) In general.
The schedule of fees for services performed in responding to requests for records is as follows:

[TABLE NOT INCLUDED]

(2) Application of schedule.
Personnel search time includes time expended in manual paper records searches, indices searches, review of computer search results for relevance, and personal computer system searches. In any event where the actual cost to ODNI of a particular item is less than the above schedule (e.g., a large production run of a document resulting in a cost less than $5.00 per hundred pages), then the actual lesser cost will be charged.

(3) Other services.
For all other types of output, production, or reproduction (e.g., photographs, maps, or published reports), ODNI will charge actual cost or amounts authorized by statute. Determinations of actual cost shall include the commercial cost of the media, the personnel time expended in making the item to be released, and an allocated cost of the equipment used in making the item, or, if the production is effected by a commercial service, then that charge shall be deemed the actual cost for purposes of this regulation.

(h) Limitations on collection of fees

(1) In general.
No fees will be charged if the cost of collecting the fee is equal to or greater than the fee itself. That cost includes the administrative costs to ODNI of billing, receiving, recording, and processing the fee for deposit to the Treasury Department and, as of the date of these regulations, is deemed to be $10.00.

(i) Fee categories.

There are four categories of FOIA requesters for fee purposes: Commercial use requesters, educational and non-commercial scientific institution requesters, representatives of the news media requesters, and all other requesters. The categories are defined in § 1700.2 and applicable fees will be assessed as follows:
(1) Commercial use requesters: Charges which recover the full direct costs of searching for, reviewing, and duplicating responsive records (if any);
(2) Educational and non-commercial scientific institution requesters, and representatives of the news media requesters: Only charges for reproduction beyond the first 100 pages;
(3) All other requesters: Charges which recover the full direct cost of searching for and reproducing responsive records (if any) beyond the first 100 pages of reproduction and the first two hours of search time which will be furnished without charge.

(j) Associated requests.

If it appears a requester or a group of requesters acting in concert have requested portions of an apparently unitary request for the purpose of avoiding the assessment of fees, ODNI may aggregate any such requests and charge accordingly. Requests from multiple requesters will not be aggregated without clear evidence. ODNI will not aggregate multiple unrelated requests.
32 CFR Section 1700.7: Processing of requests for records.

(a) In general.

Requests meeting the requirements of § 1700.3 through § 1700.6 shall be accepted as formal requests and processed under the FOIA and this Part. A request will not be considered received until it reaches the IMO. Ordinarily upon its receipt a request will be date-stamped as received. It is this date that establishes when your request is received for administrative purposes, not any earlier date such as the date of the letter or its postmark date. For the quickest possible handling, both the request letter and the envelope should be marked “Freedom of Information Act Request.”

(b) Electronic Reading Room.

ODNI maintains an online FOIA Reading Room on the ODNI Web site which contains the information that the FOIA requires be routinely made available for public inspection and copying as well as other information determined to be of general public interest.

(c) Confirming the existence of certain documents.

In processing a request, ODNI shall decline to confirm or deny the existence of responsive records whenever the fact of their existence or nonexistence is itself classified under Executive Order 12,958 and its amending orders, reveals intelligence sources and methods protected pursuant to 50 U.S.C. 403-1(i)(1), or would be an invasion of the personal privacy of third parties. In such circumstances, ODNI, in its final written response, shall so inform the requester and advise of his or her right to file an administrative appeal.

(d) Time for response.

Whenever the statutory time limits for processing a request cannot be met because of “unusual circumstances,” as defined in the FOIA, and the component determines to extend the time limits on that basis, ODNI will inform the requester in writing and advise the requester of the right to narrow the scope of his or her request or agree to an alternative timeframe for processing.

(e) Multitrack processing.

ODNI may use two or more processing tracks by distinguishing between simple and more complex requests based on the amount of work and/or time needed to process the request, including through limits based on the number of pages involved. ODNI may provide requesters in its slower track with an opportunity to limit the scope of their requests in order to qualify for faster processing within the specified limits of its faster track.
32 CFR Section 1700.8: Action on the request.

(a) Initial action for access.

ODNI staff identified to search for records pursuant to a FOIA request shall search all relevant record systems within their cognizance as of the date the search is commenced. A staff member tasked to conduct a search shall:

(1) Determine whether records exist;
(2) Determine whether and to what extent any FOIA exemptions apply;
(3) Make recommendations for withholding records or portions of records that originated in the staff member's organization and for which there is a legal basis for denial or make a recommendation in accordance with § 1700.7(c). In making recommendations, ODNI staff shall be guided by the procedures specified in § 1700.10 regarding confidential commercial information and § 1700.11 regarding third party information; and
(4) Forward to the Director, IMO, all records responsive to the request.

(b) Referrals and consultations.

ODNI records containing information originated by other ODNI components shall be forwarded to those entities for action in accordance with paragraph (a) of this section and returned. Records originated by other federal agencies or ODNI records containing other federal agency information shall be forwarded to such agencies for processing and direct response to the requester or for consultation and return to the ODNI. ODNI will notify the requester if it makes a referral for direct response.

(c) Release of information.

When the Director, IMO (or Appeals Authority) makes a final determination to release records, the records will be forwarded to the requester in an appropriate format promptly upon compliance with any preliminary procedural requirements, including payment of fees. If any portion of a record is withheld initially or upon appeal, the Director, IMO (or Appeals Authority) will provide a written response that shall include, at a minimum:

(1) The basis for the withholding, citing the specific statutory exemption or exemptions invoked under the FOIA with respect to each portion withheld, unless documents are withheld in accordance with § 1700.7(c);
(2) When the withholding is based in whole or in part on a security classification, the explanation shall include a determination that the record meets the cited criteria and rationale of the governing Executive Order;
(3) When the denial is based on 5 U.S.C. 552(b)(3), the statute relied upon; and
(4) Notice to the requester of the right to judicial review.

32 CFR Section 1700.9: Payment of fees, notification of decision, and right of appeal.
(a) Fees in general.

Fees collected under this part do not accrue to ODNI and shall be deposited immediately to the general account of the United States Treasury.

(b) Notification of decision.

Upon completion of all required review and the receipt of accrued fees (or promise to pay such fees), ODNI will promptly inform the requester in writing of those records or portions of records that will be released and those that will be denied.

1. For documents to be released, ODNI will provide paper copies or documents on electronic media, if requested and available;
2. For documents not released or partially released, ODNI shall explain the reasons for any denial and give notice of a right of administrative appeal. For partial releases, redactions will be made to ensure requesters can see the placement and general length of redactions with the applicable exemption or exemptions clearly with respect to each redaction.

32 CFR Section 1700.10: Procedures for business information.

(a) In general.

Business information obtained by ODNI from a submitter shall not be disclosed pursuant to a FOIA request except in accordance with this section. For purposes of this section, the following definitions apply:

1. Business information means commercial or financial information in which a legal entity has a recognized property interest;

2. Confidential commercial information means such business information provided to the United States Government by a submitter which is reasonably believed to contain information exempt from release under Exemption 4 of the FOIA, 5 U.S.C. 552(b)(4), because disclosure could reasonably be expected to cause substantial competitive harm; and

3. Submitter means any person or entity who provides confidential commercial information to the United States Government; it includes, but is not limited to, corporations, businesses (however organized), State governments, and foreign governments.

(b) Designation of confidential commercial information.

A submitter of business information will use good-faith efforts to designate, by appropriate markings, either at the time of submission or at a reasonable time thereafter, any portions of its submission that it considers to be confidential commercial information and hence protected from required disclosure pursuant
to Exemption 4 of the FOIA. Such designations shall expire 10 years after the date of the submission unless the submitter requests, and provides justification for, a longer designation period.

(c) Process in event of FOIA request

(1) Notice to submitters.
ODNI shall provide a submitter with prompt written notice of receipt of a FOIA request encompassing business information whenever:
(i) The submitter has in good faith designated the information as confidential commercial information, or
(ii) ODNI staff believe that disclosure of the information could reasonably be expected to cause substantial competitive harm, and
(iii) The information was submitted within the last 10 years unless the submitter requested and provided acceptable justification for a specific notice period of greater duration.

(2) Form of notice.
Communication to a submitter of commercial information shall either describe the exact nature of the confidential commercial information at issue or provide copies of the responsive records containing such information.

(3) Response by submitter.
(i) Within seven days of the notice described in paragraph (c)(1), all claims of confidentiality by a submitter must be supported by a detailed statement of any objection to disclosure. Such statement shall:
(A) Affirm that the information has not been disclosed to the public;
(B) Explain why the information is a trade secret or confidential commercial information;
(C) Explain in detail how disclosure of the information will result in substantial competitive harm;
(D) Affirm that the submitter will provide ODNI and the Department of Justice with such litigation support as requested; and
(E) Be certified by an officer authorized to legally bind the submitter.
(ii) It should be noted that information provided by a submitter pursuant to this provision may itself be subject to disclosure under the FOIA.

(4) Decision and notice of intent to disclose.
(i) ODNI shall consider carefully a submitter's objections and specific grounds for nondisclosure prior to its final determination. If the Director, IMO, decides to disclose a document over the objection of a submitter, ODNI shall provide the submitter a written notice that shall include:
(A) A statement of the reasons for which the submitter's disclosure objections were not sustained;
(B) A description of the information to be disclosed; and
(C) A specified disclosure date that is seven days after the date of the instant notice.
(ii) When notice is given to a submitter under this section, the ODNI shall also notify the requester and, if the ODNI notifies a submitter that it intends to disclose information, then the requester shall be notified also and given the proposed date for disclosure.

(5) Notice of FOIA lawsuit.
If a requester initiates legal action seeking to compel disclosure of information asserted to be within the scope of this section, ODNI shall promptly notify the submitter. The submitter, as specified above, shall provide such litigation assistance as required by ODNI and the Department of Justice.

(6) Exceptions to notice requirement.
The notice requirements of this section shall not apply if ODNI determines that:
(i) The information should not be disclosed, pursuant to Exemption 4 and/or any other exemption of the FOIA;
(ii) The information has been published lawfully or has been officially made available to the public;
(iii) The disclosure of the information is otherwise required by law or federal regulation; or
(iv) The designation made by the submitter under this section appears frivolous, except that, in such a case, the ODNI will, within a reasonable time prior to the specified disclosure date, give the submitter written notice of any final decision to disclose the information.

32 CFR Section 1700.11: Procedures for information concerning other persons.

(a) In general.

Personal information concerning individuals other than the requester shall not be disclosed under the FOIA if the proposed release would constitute a clearly unwarranted invasion of personal privacy, or, if the information was compiled for law enforcement purposes, it could reasonably be expected to constitute an unwarranted invasion of personal privacy. See 5 U.S.C. 552 (b)(6) and (b)(7)(C).

For purposes of this section, the following definitions apply:
(1) Personal information means any information about an individual that is not a matter of public record, or easily discernible to the public, or protected from disclosure because of the implications that arise from Government possession of such information.
(2) Public interest means the public interest in understanding the operations and activities of the United States Government and not simply any matter that might be of general interest to the requester or members of the public.

(b) Determination to be made.

In making the required determination under this section and pursuant to Exemptions 6 and 7(C) of the FOIA, ODNI will balance the privacy interests that
would be compromised by disclosure against the public interest in release of the requested information.

(c) Otherwise.

A requester seeking information on a third party is encouraged to provide a signed affidavit or declaration from the third party consenting to disclosure of the information. However, any such statements shall be narrowly construed and the Director, IMO, in the exercise of that officer's discretion and administrative authority, may seek clarification from the third party prior to any or all releases.

32 CFR Section 1700.12: Requests for expedited processing.

(a) In general.

All requests will be handled in the order received on a strictly “first-in, first-out” basis. Exceptions to this rule will only be made in accordance with the following procedures.

(b) Procedure.

A requester who seeks expedited processing must submit a statement, certified to be true and correct, explaining in detail the basis for requesting expedited processing. Within ten calendar days of its receipt of a request for expedited processing, the IMO shall decide whether to grant it and shall notify the requester of the decision. If a request for expedited processing is granted, the request shall be given priority and shall be processed as soon as practicable.

(c) Determination to be made:

Requests and appeals will be taken out of order and given expedited processing treatment whenever it is determined that they involve:
(1) Circumstances in which the lack of expedited treatment could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or
(2) An urgency to inform the public concerning an actual or alleged Federal Government activity, if made by a person primarily engaged in disseminating information.

32 CFR Section 1700.13: Right to appeal and appeal procedures.

(a) Right to appeal.

Individuals who disagree with a decision not to produce a document or parts of a document, to deny a fee category request, to deny a request for a fee waiver or fee reduction, to deny expedited processing, or a decision regarding a fee estimate or
a determination that no records exist, should submit a written request for review to the Chief FOIA Officer c/o Director, Information Management Office, Office of the Director of National Intelligence, Washington, DC 20511. The words “FOIA APPEAL” should be written on the letter and the envelope. The appeal must be signed by the individual or his legal counsel.

(b) Requirements as to time and form.

Appeals of adverse decisions must be received within 45 days of the date of the ODNI’s initial decision. Requesters should include a statement of the reasons supporting the request for reversal of the initial decision.

(c) Exceptions.

No appeal shall be accepted if the requester has outstanding fees for information services at this or another federal agency. In addition, no appeal shall be accepted if the information in question has been the subject of an administrative review within the previous two years or is the subject of pending litigation in the Federal courts.

32 CFR Section 1700.14: Action by appeals authority.
(a) The Director of the Intelligence Staff, after consultation with any ODNI component organization involved in the initial decision as well as with the Office of General Counsel, will make a final determination on the appeal. Appeals of denials of requests for expedited processing shall be acted on expeditiously.
(b) The Director, IMO, will ordinarily be the initial deciding official on FOIA requests to the ODNI. However, in the event the Director of the Intelligence Staff makes an initial decision that is later appealed, the Principal Deputy Director for National Intelligence will decide the appeal in accordance with the procedures in this section.
32 CFR PART 1701—ADMINISTRATION OF RECORDS UNDER THE PRIVACY ACT OF 1974

➢ Subpart A—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974
  o 1701.1: Purpose, scope, applicability.
  o 1701.2: Definitions.
  o 1701.3: Contact for general information and requests.
  o 1701.4: Privacy Act responsibilities/policy.
  o 1701.5: Collection and maintenance of records.
  o 1701.6: Disclosure of records/policy.
  o 1701.7: Requests for notification of and access to records.
  o 1701.8: Requests to amend or correct records.
  o 1701.9: Requests for an accounting of record disclosures.
  o 1701.10: ODNI responsibility for responding to access requests.
  o 1701.11: ODNI responsibility for responding to requests for amendment or correction.
  o 1701.12: ODNI responsibility for responding to requests for accounting.
  o 1701.13: Special procedures for medical/psychiatric/psychological testing records.
  o 1701.14: Appeals.
  o 1701.15: Fees.
  o 1701.16: Contractors.
  o 1701.17: Standards of conduct.

➢ Subpart B—Exemption of Records Systems Under the Privacy Act
  o 1701.20: Exemption policies.
  o 1701.21: Exemption of National Counterterrorism Center (NCTC) systems of records.
  o 1701.22: Exemption of Office of the National Counterintelligence Executive (ONCIX) systems of records.
  o 1701.24: Exemption of Office of the Director of National Intelligence (ODNI) systems of records.

➢ Subpart C—Routine Uses Applicable to More Than One ODNI System of Records
  o 1701.30: Policy and applicability.
  o 1701.31: General routine uses.
Authority:

Source:
73 FR 16532, Mar. 28, 2008, unless otherwise noted.
SUBPART A—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974

32 CFR Section 1701.1: Purpose, scope, applicability.

(a) Purpose.

This subpart establishes the policies and procedures the Office of the Director of National Intelligence (ODNI) will follow in implementing the requirements of the Privacy Act of 1974, 5 U.S.C. 552a, as amended. This subpart sets forth the procedures ODNI must follow in collecting and maintaining personal information from or about individuals, as well as procedures by which individuals may request to access or amend records about themselves and request an accounting of disclosures of those records by the ODNI. In addition, this subpart details parameters for disclosing personally identifiable information to persons other than the subject of a record.

(b) Scope.

The provisions of this subpart apply to all records in systems of records maintained by ODNI directorates, centers, mission managers and other sub-organizations [hereinafter called “components”] that are retrieved by an individual's name or personal identifier.

(c) Applicability.

This subpart governs the following individuals and entities:
(1) All ODNI staff and components must comply with this subpart. The terms “staff” and “component” are defined in § 1701.2.
(2) Unless specifically exempted, this subpart also applies to advisory committees and councils within the meaning of the Federal Advisory Committee Act (FACA) which provide advice to: Any official or component of ODNI; or the President, and for which ODNI has been delegated responsibility for providing service.

(d) Relation to Freedom of Information Act.

The ODNI shall provide a subject individual under this subpart all records which are otherwise accessible to such individual under the provisions of the Freedom of Information Act, 5 U.S.C. 552.

32 CFR Section 1701.2: Definitions.
For purposes of this subpart, the following terms have the meanings indicated:

Access

means making a record available to a subject individual.
Act

means the Privacy Act of 1974.

Agency

means the ODNI or any of its components.

Component

means any directorate, mission manager, or other sub-organization in the ODNI or reporting to the Director, that has been designated or established in the ODNI pursuant to Section 103 of the National Security Act of 1947, as amended, including the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC) and the Office of the National Counterintelligence Executive (ONCIX), or such other offices and officials as may be established by law or as the Director may establish or designate in the ODNI, for example, the Program Manager, Information Sharing Environment (ISE) and the Inspector General (IG).

Disclosure

means making a record about an individual available to or releasing it to another party.

FOIA

means the Freedom of Information Act.

Individual

, when used in connection with the Privacy Act, means a living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. It does not include sole proprietorships, partnerships, or corporations.

Information

means information about an individual and includes, but is not limited to, vital statistics; race, sex, or other physical characteristics; earnings information; professional fees paid to an individual and other financial information; benefit
data or claims information; the Social Security number, employer identification number, or other individual identifier; address; phone number; medical information; and information about marital, family or other personal relationships.

Maintain

means to establish, collect, use, or disseminate when used in connection with the term record; and, to have control over or responsibility for a system of records, when used in connection with the term system of records.

Notification

means communication to an individual whether he is a subject individual.

Office of the Director of National Intelligence

means any and all of the components of the ODNI.

Record

means any item, collection, or grouping of information about an individual that is maintained by the ODNI including, but not limited to, information such as an individual's education, financial transactions, medical history, and criminal or employment history that contains the individual's name, or an identifying number, symbol, or any other identifier assigned to an individual. When used in this subpart, record means only a record that is in a system of records.

Routine

use means the disclosure of a record outside ODNI, without the consent of the subject individual, for a purpose which is compatible with the purpose for which the record was collected. It does not include disclosure which the Privacy Act otherwise permits pursuant to subsection (b) of the Act.

Staff

means any current or former regular or special employee, detailee, assignee, employee of a contracting organization, or independent contractor of the ODNI or any of its components.
individual means the person to whom a record pertains (or “record subject”).

System of records

means a group of records under ODNI's control from which information about an individual is retrieved by the name of the individual or by an identifying number, symbol, or other particular assigned to the individual. Single records or groups of records which are not retrieved by a personal identifier are not part of a system of records,

32 CFR Section 1701.3: Contact for general information and requests.
Privacy Act requests and appeals and inquiries regarding this subpart or about ODNI’s Privacy Act program must be submitted in writing to the Director, Information Management Office (D/IMO), Office of the Director of National Intelligence, Washington, DC 20511 (by mail or by facsimile at 703-482-2144) or to the contact designated in the specific Privacy Act System of Records Notice. Privacy Act requests with the required identification statement and signature pursuant to paragraphs (d) and (e) of § 1701.7 of this subpart must be filed in original form.

32 CFR Section 1701.4: Privacy Act responsibilities/policy.
The ODNI will administer records about individuals consistent with statutory, administrative, and program responsibilities. Subject to exemptions authorized by the Act, ODNI will collect, maintain and disclose records as required and will honor subjects' rights to view and amend records and to obtain an accounting of disclosures.

32 CFR Section 1701.5: Collection and maintenance of records.
(a) ODNI will not maintain a record unless:
(1) It is relevant and necessary to accomplish an ODNI function required by statute or Executive Order;
(2) It is acquired to the greatest extent practicable from the subject individual when ODNI may use the record to make any determination about the individual;
(3) The individual providing the record is informed of the authority for providing the record (including whether providing the record is mandatory or voluntary), the principal purpose for maintaining the record, the routine uses for the record, and what effect refusing to provide the record may have;
(4) It is maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual in the determination;
(b) Except as to disclosures made to an agency or made under the FOIA, ODNI will make reasonable efforts prior to disseminating a record about an individual, to ensure that the record is accurate, relevant, timely, and complete;
(c) ODNI will not maintain or develop a system of records that is not the subject of a current or planned public notice;
(d) ODNI will not adopt a routine use of information in a system without notice and invitation to comment published in the Federal Register at least 30 days prior to final adoption of the routine use;
(e) To the extent ODNI participates with a non-Federal agency in matching activities covered by section (8) of the Act, ODNI will publish notice of the matching program in the Federal Register;
(f) ODNI will not maintain a record which describes how an individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the subject individual, or unless pertinent to and within the scope of an authorized law enforcement activity;
(g) When required by the Act, ODNI will maintain an accounting of all disclosures of records by the ODNI to persons, organizations or agencies;
(h) Each ODNI component shall implement administrative, physical and technical controls to prevent unauthorized access to its systems of records, to prevent unauthorized disclosure of records, and to prevent physical damage to or destruction of records;
(i) ODNI will establish rules and instructions for complying with the requirements of the Privacy Act, including notice of the penalties for non-compliance, applicable to all persons involved in the design, development, operation or maintenance of any system of records.

32 CFR Section 1701.6: Disclosure of records/policy.
Consistent with 5 U.S.C. 552a(b), ODNI will not disclose any record which is contained in a system of records by any means (written, oral or electronic) without the consent of the subject individual unless disclosure without consent is made for reasons permitted under applicable law, including:
(a) Internal agency use on a need-to-know basis;
(b) Release under the Freedom of Information Act (FOIA) if not subject to protection under the FOIA exemptions;
(c) A specific “routine use” as described in the ODNI’s published compilation of Routine Uses Applicable to More Than One ODNI System of Records or in specific published Privacy Act Systems of Records Notices (available at http://www.dni.gov);
(d) Release to the Bureau of the Census, the National Archives and Records Administration, or the Government Accountability Office, for the performance of those entities' statutory duties;
(e) Release in non-identifiable form to a recipient who has provided written assurance that the record will be used solely for statistical research or reporting;
(f) Compelling circumstances in which the health or safety of an individual is at risk;
(g) Release pursuant to the order of a court of competent jurisdiction or to a governmental entity for a specifically documented civil or criminal law enforcement activity;
(h) Release to either House of Congress or to any committee, subcommittee or joint committee thereof to the extent of matter within its jurisdiction;
(i) Release to a consumer reporting agency in accordance with section 3711(e) of Title 31.

32 CFR Section 1701.7: Requests for notification of and access to records.

(a) How to request.

Unless records are not subject to access (see paragraph (b) of this section), individuals seeking access to records about themselves may submit a request in writing to the D/IMO, as directed in Sec. 1701.3 of this subpart, or to the contact designated in the specific Privacy Act System of Records Notice. To ensure proper routing and tracking, requesters should mark the envelope “Privacy Act Request.”

(b) Records not subject to access.

The following records are not subject to review by subject individuals:
(1) Records in ODN systems of records that ODNI has exempted from access and correction under the Privacy Act, 5 U.S.C. 552a(j) or (k), by notice published in the Federal Register, or where those exemptions require that ODNI can neither confirm nor deny the existence or nonexistence of responsive records (see § 1701.10(c)(iii)).
(2) Records in ODNI systems of records that another agency has exempted from access and correction under the Privacy Act, 5 U.S.C. 552a(j) or (k), by notice published in the Federal Register, or where those exemptions require that ODNI can neither confirm nor deny the existence or nonexistence of responsive records (see § 1701.10(c)(iii)).

(c) Description of records.

Individuals requesting access to records about themselves should, to the extent possible, describe the nature of the records, why and under what circumstances the requester believes ODNI maintains the records, the time period in which they may have been compiled and, ideally, the name or identifying number of each Privacy Act System of Records in which they might be included. The ODNI publishes notices in the Federal Register that describe its systems of records. The Federal Register compiles these notices biennially and makes them available in hard copy at large reference libraries and in electronic form at the Government Printing Office’s World Wide Web site, http://www.gpoaccess.gov.

(d) Verification of identity.
A written request for access to records about oneself must include full (legal) name, current address, date and place of birth, and citizenship status. Aliens lawfully admitted for permanent residence must provide their Alien Registration Number and the date that status was acquired. The D/IMO may request additional or clarifying information to ascertain identity. Access requests must be signed and the signature either notarized or submitted under 28 U.S.C. 1746, authorizing statements made under penalty of perjury as a substitute for notarization.

(e) Verification of guardianship or representational relationship.

The parent or guardian of a minor, the guardian of an individual under judicial disability, or an attorney retained to represent an individual shall provide, in addition to establishing the identity of the minor or individual represented as required in paragraph (d) of this section, evidence of such representation by submitting a certified copy of the minor's birth certificate, court order, or representational agreement which establishes the relationship and the requester's identity.

(f) ODNI will permit access to or provide copies of records to individuals other than the record subject (or the subject's legal representative) only with the requester's written authorization.

32 CFR Section 1701.8: Requests to amend or correct records.

(a) How to request.

Unless the record is not subject to amendment or correction (see paragraph (b) of this section), individuals (or guardians or representatives acting on their behalf) may make a written amendment or correction request to the D/IMO, as directed in § 1701.3 of this subpart, or to the contact designated in a specific Privacy Act System of Records. Requesters seeking amendment or correction should identify the particular record or portion subject to the request, explain why an amendment or correction is necessary, and provide the desired replacement language. Requesters may submit documentation supporting the request to amend or correct. Requests for amendment or correction will lapse (but may be re-initiated with a new request) if all necessary information is not submitted within forty-five (45) days of the date of the original request. The identity verification procedures of paragraphs (d) and (e) of § 1701.7 of this subpart apply to amendment requests.

(b). (1) Records which are determinations of fact or evidence received (e.g., transcripts of testimony given under oath or written statements made under oath; transcripts of grand jury proceedings, judicial proceedings, or quasi-judicial proceedings, which are the official record of those proceedings; pre-sentence records that originated with the courts) and
(2) Records in ODNI systems of records that ODNI or another agency has exempted from amendment and correction under Privacy Act, 5 U.S.C. 552a(j) or (k) by notice published in the Federal Register.

32 CFR Section 1701.9: Requests for an accounting of record disclosures.

(a) How to request.

Except where accountings of disclosures are not required to be kept (see paragraph (b) of this section), record subjects (or their guardians or representatives) may request an accounting of disclosures that have been made to another person, organization, or agency as permitted by the Privacy Act at 5 U.S.C. 552a(b). This accounting contains the date, nature, and purpose of each disclosure, as well as the name and address of the person, organization, or agency to which the disclosure was made. Requests for accounting should identify each record in question and must be made in writing to the D/IMO, as indicated in § 1701.3 of this subpart, or to the contact designated in a specific Privacy Act System of Records.

(b) Accounting not required.

The ODNI is not required to provide accounting of disclosure in the following circumstances:
(1) Disclosures for which the Privacy Act does not require accounting, i.e., disclosures to employees within the agency and disclosures made under the FOIA;
(2) Disclosures made to law enforcement agencies for authorized law enforcement activities in response to written requests from the respective head of the law enforcement agency specifying the law enforcement activities for which the disclosures are sought; or
(3) Disclosures from systems of records that have been exempted from accounting requirements under the Privacy Act, 5 U.S.C. 552a(j) or (k), by notice published in the Federal Register.

32 CFR Section 1701.10: ODNI responsibility for responding to access requests.

(a) Acknowledgement of requests.

Upon receipt of a request providing all necessary information, the D/IMO shall acknowledge receipt to the requester and provide an assigned request number for further reference.

(b) Tasking to component.
Upon receipt of a proper access request, the D/IMO shall provide a copy of the request to the point of contact (POC) in the ODNI component with which the records sought reside. The POC within the component shall determine whether responsive records exist and, if so, recommend to the D/IMO:
(1) Whether access should be denied in whole or part (and the legal basis for denial under the Privacy Act); or
(2) Whether coordination with or referral to another component or federal agency is appropriate.

(c) Coordination and referrals

(1) Examination of records.
If a component POC receiving a request for access determines that an originating agency or other agency that has a substantial interest in the record is best able to process the request (e.g., the record is governed by another agency's regulation, or another agency originally generated or classified the record), the POC shall forward to the D/IMO all records necessary for coordination with or referral to the other component or agency, as well as specific recommendations with respect to any denials.

(2) Notice of referral.
Whenever the D/IMO refers all or any part of the responsibility for responding to a request to another agency, the D/IMO shall notify the requester of the referral.

(3) Effect of certain exemptions.
(i) In processing a request, the ODNI shall decline to confirm or deny the existence or nonexistence of any responsive records whenever the fact of their existence or nonexistence:
(A) May reveal protected intelligence sources and collection methods (50 U.S.C. 403-1(i)); or
(B) Is classified and subject to an exemption appropriately invoked by ODNI or another agency under subsections (j) or (k) of the Privacy Act.
(ii) In such event, the ODNI will inform the requester in writing and advise the requestor of the right to file an administrative appeal of any adverse determination.

(d) Time for response.

The D/IMO shall respond to a request for access promptly upon receipt of recommendations from the POC and determinations resulting from any necessary coordination with or referral to another agency. The D/IMO may determine to update a requester on the status of a request that remains outstanding longer than reasonably expected.

(e) ODNI action on requests for access
(1) Grant of access.
Once the D/IMO determines to grant a request for access in whole or in part, the D/IMO shall notify the requester in writing and come to agreement with the requester about how to effect access, whether by on-site review or duplication of the records. If a requester is accompanied by another person, the requester shall be required to authorize in writing any discussion of the records in the presence of the other person.

(2) Denial of access.
The D/IMO shall notify the requester in writing when an adverse determination is made denying a request for access in any respect. Adverse determinations, or denials, consist of a determination to withhold any requested record in whole or in part; a determination that a requested record does not exist or cannot be located; a determination that what has been requested is not a record subject to the Privacy Act; or a determination that the existence of a record can neither be confirmed nor denied. The notification letter shall state:
(i) The reason(s) for the denial; and
(ii) The procedure for appeal of the denial under § 1701.14 of this subpart.

32 CFR Section 1701.11: ODNI responsibility for responding to requests for amendment or correction.

(a) Acknowledgment of request.
The D/IMO shall acknowledge receipt of a request for amendment or correction of records in writing and provide an assigned request number for further reference.

(b) Tasking of component.
Upon receipt of a proper request to amend or correct a record, the D/IMO shall forward the request to the POC in the component maintaining the record. The POC shall promptly evaluate the proposed amendment or correction in light of any supporting justification and recommend that the D/IMO grant or deny the request or, if the request involves a record subject to correction by an originating agency, refer the request to the other agency.

(c) Action on request for amendment or correction.

(1) If the POC determines that the request for amendment or correction is justified, in whole or in part, the D/IMO shall promptly:
(i) Make the amendment, in whole or in part, as requested and provide the requester a written description of the amendment or correction made; and
(ii) Provide written notice of the amendment or correction to all persons, organizations or agencies to which the record has been disclosed (if an accounting of the disclosure was made);
(2) Where the D/IMO has referred an amendment request to another agency, the D/IMO, upon confirmation from that agency that the amendment has been effected, shall provide written notice of the amendment or correction to all persons, organizations or agencies to which ODNI previously disclosed the record.

(3) If the POC determines that the requester's records are accurate, relevant, timely and complete, and that no basis exists for amending or correcting the record, either in whole or in part, the D/IMO shall inform the requester in writing of:

(i) The reason(s) for the denial; and

(ii) The procedure for appeal of the denial under Sec. 1701.15 of this subpart.

32 CFR Section 1701.12: ODNI responsibility for responding to requests for accounting.

(a) Acknowledgement of request.

Upon receipt of a request for accounting, the D/IMO shall acknowledge receipt of the request in writing and provide an assigned request number for further reference.

(b) Tasking of component.

Upon receipt of a request for accounting, the D/IMO shall forward the request to the POC in the component maintaining the record. The POC shall work with the component's information management officer and the systems administrator to generate the requested disclosure history.

(c) Action on request for accounting.

The D/IMO will notify the requester when the accounting is available for on-site review or transmission in paper or electronic medium.

(d) Notice of court-ordered disclosures.

The D/IMO shall make reasonable efforts to notify an individual whose record is disclosed pursuant to court order. Notice shall be made within a reasonable time after receipt of the order; however, when the order is not a matter of public record, the notice shall be made only after the order becomes public. Notice shall be sent to the individual’s last known address and include a copy of the order and a description of the information disclosed. No notice shall be made regarding records disclosed from a criminal law enforcement system that has been exempted from the notice requirement.

(e) Notice of emergency disclosures.
ODNI shall notify an individual whose record it discloses under compelling circumstances affecting health or safety. This notice shall be mailed to the individual's last known address and shall state the nature of the information disclosed; the person, organization, or agency to which it was disclosed; the date of disclosure; and the compelling circumstances justifying the disclosure. This provision shall not apply in circumstances involving classified records that have been exempted from disclosure pursuant to subsection (j) or (k) of the Privacy Act.

32 CFR Section 1701.13: Special procedures for medical/psychiatric/psychological records.
Current and former ODNI employees, including current and former employees of ODNI contractors, and unsuccessful applicants for employment may seek access to their medical, psychiatric or psychological testing records by writing to: Information and Privacy Coordinator, Central Intelligence Agency, Washington, DC 20505, and provide identifying information as required by paragraphs (d) and (e) of § 1701.7 of this subpart. The Central Intelligence Agency's Privacy Act Regulations will govern administration of these types of records, including appeals from adverse determinations.

32 CFR Section 1701.14: Appeals.
(a) Individuals may appeal denials of requests for access, amendment, or accounting by submitting a written request for review to the Director, Information Management Office (D/IMO) at the Office of the Director of National Intelligence, Washington, DC 20511. The words “PRIVACY ACT APPEAL” should be written on the letter and the envelope. The appeal must be signed by the record subject or legal representative. No personal appearance or hearing on appeal will be allowed.
(b) The D/IMO must receive the appeal letter within 45 calendar days of the date the requester received the notice of denial. The postmark is conclusive as to timeliness. Copies of correspondence from ODNI denying the request to access or amend the record should be included with the appeal, if possible. At a minimum, the appeal letter should identify:
(1) The records involved;
(2) The date of the initial request for access to or amendment of the record;
(3) The date of ODNI’s denial of that request; and
(4) A statement of the reasons supporting the request for reversal of the initial decision. The statement should focus on information not previously available or legal arguments demonstrating that the ODNI’s decision is improper.

(c) Following receipt of the appeal, the Director of Intelligence Staff (DIS) shall, in consultation with the Office of General Counsel, make a final determination in writing on the appeal.
(d) Where ODNI reverses an initial denial, the following procedures apply:
(1) If ODNI reverses an initial denial of access, the procedures in paragraph (e)(1) of § 1701.10 of this subpart will apply.
(2) If ODNI reverses its initial denial of a request to amend a record, the POC will ensure that the record is corrected as requested, and the D/IMO will inform the individual of the correction, as well as all persons, organizations and agencies to which ODNI had disclosed the record.

(3) If ODNI reverses its initial denial of a request for accounting, the POC will notify the requester when the accounting is available for on-site review or transmission in paper or electronic medium.

(e) If ODNI upholds its initial denial or reverses in part (i.e., only partially granting the request), ODNI's notice of final agency action will inform the requester of the following rights:

(1) Judicial review of the denial under 5 U.S.C. 552a(g)(1), as limited by 5 U.S.C. 552a(g)(5).

(2) Opportunity to file a statement of disagreement with the denial, citing the reasons for disagreeing with ODNI's final determination not to correct or amend a record. The requester's statement of disagreement should explain why he disputes the accuracy of the record.

(3) Inclusion in one's record of copies of the statement of disagreement and the final denial, which ODNI will provide to all subsequent recipients of the disputed record, as well as to all previous recipients of the record where an accounting was made of prior disclosures of the record.

32 CFR Section 1701.15: Fees.
ODNI shall charge fees for duplication of records under the Privacy Act, 5 U.S.C. 552a, in the same way in which it will charge for duplication of records under § 1700.7(g), ODNI's regulation implementing the fee provision of the Freedom of Information Act, 5 U.S.C. 552.

32 CFR Section 1701.16: Contractors.
(a) Any approved contract for the operation of a Privacy Act system of records to accomplish a function of the ODNI will contain the Privacy Act provisions prescribed by the Federal Acquisition Regulations (FAR) at 48 CFR part 24, requiring the contractor to comply with the Privacy Act and this subpart. The contracting component will be responsible for ensuring that the contractor complies with these contract requirements. This section does not apply to systems of records maintained by a contractor as a function of management discretion, e.g., the contractor's personnel records.

(b) Where the contract contains a provision requiring the contractor to comply with the Privacy Act and this subpart, the contractor and any employee of the contractor will be considered employees of the ODNI for purposes of the criminal penalties of the Act, 5 U.S.C. 552a(i).

32 CFR Section 1701.17: Standards of conduct.

(a) General.
ODNI will ensure that staff are aware of the provisions of the Privacy Act and of their responsibilities for protecting personal information that ODNI collects and maintains, consistent with Sec. 1701.5 and 1701.6 of this subpart. 

(b) Criminal penalties

(1) Unauthorized disclosure
Criminal penalties may be imposed against any ODNI staff who, by virtue of employment, has possession or access to ODNI records which contain information identifiable with an individual, the disclosure of which is prohibited by the Privacy Act or by these rules, and who, knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it.

(2) Unauthorized maintenance
Criminal penalties may be imposed against any ODNI staff who willfully maintains a system of records without meeting the requirements of subsection (e)(4) of the Privacy Act, 5 U.S.C. 552a. The D/IMO, the Civil Liberties Protection Officer, the General Counsel, and the Inspector General are authorized independently to conduct such surveys and inspect such records as necessary from time to time to ensure that these requirements are met.

(3) Unauthorized requests.
Criminal penalties may be imposed upon any person who knowingly and willfully requests or obtains any record concerning an individual from the ODNI under false pretenses.
SUBPART B—Exemption of Record Systems under the Privacy Act
32 CFR Section 1701.20: Exemption policies.

(a) General.

The DNI has determined that invoking exemptions under the Privacy Act and continuing exemptions previously asserted by agencies whose records ODNI receives is necessary: to ensure against the release of classified information essential to the national defense or foreign relations; to protect intelligence sources and methods; and to maintain the integrity and effectiveness of intelligence, investigative and law enforcement processes. Accordingly, as authorized by the Privacy Act, 5 U.S.C. 552a, subsections (j) and (k), and in accordance with the rulemaking procedures of the Administrative Procedures Act, 5 U.S.C. 553, the ODNI shall:

1. Exercise its authority pursuant to subsections (j) and (k) of the Privacy Act to exempt certain ODNI systems of records or portions of systems of records from various provisions of the Privacy Act; and
2. Continue in effect and assert all exemptions claimed under Privacy Act subsections (j) and (k) by an originating agency from which the ODNI obtains records where the purposes underlying the original exemption remain valid and necessary to protect the contents of the record.

(b) Related policies.

1. The exemptions asserted apply to records only to the extent they meet the criteria of subsections (j) and (k) of the Privacy Act, whether claimed by the ODNI or the originator of the records.
2. Discretion to supersede exemption: Where complying with a request for access or amendment would not appear to interfere with or adversely affect a counterterrorism or law enforcement interest, and unless prohibited by law, the D/IMO may exercise his discretion to waive the exemption. Discretionary waiver of an exemption with respect to a record will not obligate the ODNI to waive the exemption with respect to any other record in an exempted system of records. As a condition of such discretionary access, ODNI may impose any restrictions (e.g., concerning the location of file reviews) deemed necessary or advisable to protect the security of agency operations, information, personnel, or facilities.
3. Records in ODNI systems also are subject to protection under 50 U.S.C. 403-1(i), the provision of the National Security Act of 1947 which requires the DNI to protect intelligence sources and methods from unauthorized disclosure.

32 CFR Section 1701.21: Exemption of National Counterterrorism Center (NCTC) systems of records.

(a) The ODNI exempts the following systems of records from the requirements of subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1); (e)(4)(G), (H), (I); and (f) of the Privacy Act to the extent that information in the system is subject to exemption pursuant subsections (k)(1) and (k)(5) of the Act:
(1) NCTC Human Resources Management System (ODNI/NCTC-001).

(2) [Reserved]

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an investigative interest on the part of the ODNI or recipient agency and could result in release of properly classified national security or foreign policy information.

(2) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because affording access and amendment rights could alert the record subject to the investigative interest of intelligence or law enforcement agencies or compromise sensitive information classified in the interest of national security. In the absence of a national security basis for exemption, records in this system may be exempted from access and amendment to the extent necessary to honor promises of confidentiality to persons providing information concerning a candidate for position. Inability to maintain such confidentiality would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(3) From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible to establish relevance and necessity before all information is considered and evaluated in relation to an intelligence concern. In the absence of a national security basis for exemption under subsection (k)(1), records in this system may be exempted from the relevance requirement pursuant to subsection (k)(5) because it is not possible to determine in advance what exact information may assist in determining the qualifications and suitability of a candidate for position. Seemingly irrelevant details, when combined with other data, can provide a useful composite for determining whether a candidate should be appointed.

(4) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment, and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(5) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information, intelligence sources and methods, and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.

(6) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees)
because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject's access request.

(c) The ODNI exempts the following systems of records from the requirements of subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1); (e)(4)(G), (H), (I); and (f) of the Privacy Act to the extent that information in the system is subject to exemption pursuant to subsection (k)(1) of the Act:

(1) NCTC Access Authorization Records (ODNI/NCTC-002).
(2) NCTC Telephone Directory (ODNI/NCTC-003).
(3) NCTC Partnership Management Records (ODNI/NCTC-006).
(4) NCTC Tacit Knowledge Management Records (ODNI/NCTC-007).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an investigative interest on the part of the ODNI or recipient agency and could result in release of properly classified national security or foreign policy information.

(2) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because affording access and amendment rights could alert the record subject to the investigative interest of intelligence or law enforcement agencies or compromise sensitive information classified in the interest of national security.

(3) From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible to establish relevance and necessity before all information is considered and evaluated in relation to an intelligence concern.

(4) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(5) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information, intelligence sources and methods, and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.
(6) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees) because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject’s access request.

(e) The ODNI exempts the following systems of records from the requirements of subsections (c)(3); (d)(1), (2), (3), (4); (e)(1); (e)(4)(G), (H), (I); and (f) of the Privacy Act, to the extent that information in the system is subject to exemption pursuant to subsections (k)(1) and (k)(2) of the Act:

1. NCTC Knowledge Repository (SANCTUM) (ODNI/NCTC-004).
2. NCTC Online (ODNI/NCTC-005).
3. NCTC Terrorism Analysis Records (ODNI/NCTC-008).
4. NCTC Terrorist Identities Records (ODNI/NCTC-009).

(f) Exemptions from the particular subsections are justified for the following reasons:

1. From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an investigative interest on the part of the ODNI as well as the recipient agency and could: Result in release of properly classified national security or foreign policy information; compromise ongoing efforts to investigate a known or suspected terrorist; reveal sensitive investigative or surveillance techniques; or identify a confidential source. With this information, the record subject could frustrate counterintelligence measures; impede an investigation by destroying evidence or intimidating potential witnesses; endanger the physical safety of sources, witnesses, and law enforcement and intelligence personnel and their families; or evade apprehension or prosecution by law enforcement personnel.

2. From subsections (d)(1), (2), (3) and (4) (record subject’s right to access and amend records) because these provisions concern individual access to and amendment of counterterrorism, investigatory and intelligence records. Affording access and amendment rights could alert the record subject to the fact and nature of an investigation or the investigative interest of intelligence or law enforcement agencies; permit the subject to frustrate such investigation, surveillance or potential prosecution; compromise sensitive information classified in the interest of national security; identify a confidential source or disclose information which would reveal a sensitive investigative or intelligence technique; and endanger the health or safety of law enforcement personnel, confidential informants, and witnesses. In addition, affording subjects access and amendment rights would impose an impossible administrative burden to continuously reexamine investigations, analyses, and reports.

3. From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible for intelligence or law enforcement agencies to
know in advance what information about an encounter with a known or suspected terrorist will be relevant for the purpose of conducting an operational response. Relevance and necessity are questions of judgment and timing, and only after information is evaluated can relevance and necessity be established. In addition, information in the system of records may relate to matters under the investigative jurisdiction of another agency, and may not readily be segregated. Furthermore, information in these systems of records, over time, aid in establishing patterns of criminal activity that can provide leads for other law enforcement agencies.

(4) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(5) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information. Additionally, exemption from this provision is necessary to protect the privacy and safety of witnesses and sources of information, including intelligence sources and methods and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.

(6) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records and for assessing fees) because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject's access request.

32 CFR Section 1701.22: Exemption of Office of the National Counterintelligence Executive (ONCIX) system of records.

(a) The ODNI exempts the following system of records from the requirements of subsections (c)(3); (d)(1), (2), (3), (4); (e)(1); (e)(4)(G), (H), (I); and (f) of the Privacy Act, to the extent that information in the system is subject to exemption pursuant to subsections (k)(1) and (k)(2) of the Act:

(1) ONCIX Counterintelligence Damage Assessment Records (ODNI/ONCIX-001).

(2) [Reserved]
(b) Exemptions from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an investigative interest on the part of the ODNI as well as the recipient agency and could: result in release of properly classified national security or foreign policy information; compromise ongoing efforts to investigate a known or suspected terrorist; reveal sensitive investigative or surveillance techniques; or identify a confidential source. With this information, the record subject could frustrate counterintelligence measures; impede an investigation by destroying evidence or intimidating potential witnesses; endanger the physical safety of sources, witnesses, and law enforcement and intelligence personnel and their families; or evade apprehension or prosecution by law enforcement personnel.

(2) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because these provisions concern individual access to and amendment of counterterrorism, investigatory and intelligence records. Affording access and amendment rights could alert the record subject to the fact and nature of an investigation or the investigative interest of intelligence or law enforcement agencies; permit the subject to frustrate such investigation, surveillance or potential prosecution; compromise sensitive information classified in the interest of national security; identify a confidential source or disclose information which would reveal a sensitive investigative or intelligence technique; and endanger the health or safety of law enforcement personnel, confidential informants, and witnesses. In addition, affording subjects access and amendment rights would impose an impossible administrative burden to continuously reexamine investigations, analyses, and reports.

(3) From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible to know in advance what information will be relevant to evaluate and mitigate damage to the national security. Relevance and necessity are questions of judgment and timing, and only after information is evaluated can relevance and necessity be established. In addition, information in the system of records may relate to matters under the investigative jurisdiction of another agency, and may not readily be segregated. Furthermore, information in these systems of records, over time, aid in establishing patterns of criminal activity that can provide leads for other law enforcement agencies.

(4) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects to the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(5) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly
classified national defense or foreign policy information. Additionally, exemption from this provision is necessary to protect the privacy and safety of witnesses and sources of information, including intelligence sources and methods and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.

(6) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records and for assessing fees) because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject's access request.


(a) The ODNI exempts the following systems of records from the requirements of subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1); (e)(4)(G), (H), (I); and (f) of the Privacy Act to the extent that information in the system is subject to exemption pursuant subsections (k)(1) and (k)(5) of the Act:

(1) OIG Human Resources Records (ODNI/OIG-001).
(2) OIG Experts Contact Records (ODNI/OIG-002).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an investigative interest on the part of the ODNI or recipient agency and could result in release of properly classified national security or foreign policy information.

(2) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because affording access and amendment rights could alert the record subject to the investigative interest of intelligence or law enforcement agencies or compromise sensitive information classified in the interest of national security. In the absence of a national security basis for exemption under subsection (k)(1), records in this system may be exempted from access and amendment pursuant to subsection (k)(5) to the extent necessary to honor promises of confidentiality to persons providing information concerning a candidate for position. Inability to maintain such confidentiality would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(3) From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible to establish relevance and necessity before all
information is considered and evaluated in relation to an intelligence concern. In the absence of a national security basis for exemption under subsection (k)(1), records in this system may be exempted from the relevance requirement pursuant to subsection (k)(5) because it is not always possible to determine in advance what exact information may assist in determining the qualifications and suitability of a candidate for position. Seemingly irrelevant details, when combined with other data, can provide a useful composite for determining whether a candidate should be appointed.

(4) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published such a notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(5) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information, intelligence sources and methods and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.

(6) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records and for assessing fees) because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject's access request.

(c) The ODNI exempts the following system of records from the requirements of subsections (c)(3) and (4); (d)(1), (2), (3), (4); (e)(1), (2), (3), (5), (8) and (12); and (g) of the Privacy Act, to the extent that information in the system is subject to exemption pursuant to subsection (j)(2) of the Act. In addition, the following system of records is exempted from the requirements of subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1); (e)(4)(G), (H) and (I); and (f) of the Privacy Act, to the extent that information in the system is subject to exemption pursuant to subsections (k)(1) and (k)(2) of the Act.

(1) OIG Investigation and Interview Records (ODNI/OIG-003).

(2) [Reserved]

(d) Exemptions from the particular subsections are justified for the following reasons:
(1) From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an investigative interest on the part of the ODNI as well as the recipient agency and could: result in release of properly classified national security or foreign policy information; compromise ongoing efforts to investigate a known or suspected terrorist; reveal sensitive investigative or surveillance techniques; or identify a confidential source. With this information, the record subject could frustrate counterintelligence measures; impede an investigation by destroying evidence or intimidating potential witnesses; endanger the physical safety of sources, witnesses, and law enforcement and intelligence personnel and their families; or evade apprehension or prosecution by law enforcement personnel.

(2) From subsection (c)(4) (notice of amendment to record recipients) because the system is exempted from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3) and (4) (record subject’s right to access and amend records) because these provisions concern individual access to and amendment of counterterrorism, investigatory and intelligence records. Affording access and amendment rights could alert the record subject to the fact and nature of an investigation or the investigative interest of intelligence or law enforcement agencies; permit the subject to frustrate such investigation, surveillance or potential prosecution; compromise sensitive information classified in the interest of national security; identify a confidential source or disclose information which would reveal a sensitive investigative or intelligence technique; and endanger the health or safety of law enforcement personnel, confidential informants, and witnesses. In addition, affording subjects access and amendment rights would impose an impossible administrative burden to continuously reexamine investigations, analyses, and reports.

(4) From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible to know in advance what information will be relevant for the purpose of conducting an investigation. Relevance and necessity are questions of judgment and timing, and only after information is evaluated can relevance and necessity be established. In addition, information in the system of records may relate to matters under the investigative jurisdiction of another agency, and may not readily be segregated. Furthermore, information in these systems of records, over time, aid in establishing patterns of criminal activity that can provide leads for other law enforcement agencies.

(5) From subsection (e)(2) (collection directly from the individual) because application of this provision would alert the subject of a counterterrorism investigation, study or analysis to that fact, permitting the subject to frustrate or impede the activity. Counterterrorism investigations necessarily rely on information obtained from third parties rather than information furnished by subjects themselves.

(6) From subsection (e)(3) (provide Privacy Act Statement to subjects furnishing information) because the system is exempted from the (e)(2) requirement to collect information directly from the subject.
(7) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(8) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information. Additionally, exemption from this provision is necessary to protect the privacy and safety of witnesses and sources of information, including intelligence sources and methods and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.

(9) From subsection (e)(5) (maintain timely, accurate, complete and up-to-date records) because many of the records in the system are derived from other domestic and foreign agency record systems over which ODNI exercises no control. In addition, in collecting information for counterterrorism, intelligence, and law enforcement purposes, it is not possible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time and the development of additional facts and circumstances, seemingly irrelevant or dated information may acquire significance. The restrictions imposed by (e)(5) would limit the ability of intelligence analysts to exercise judgment in conducting investigations and impede development of intelligence necessary for effective counterterrorism and law enforcement efforts.

(10) From subsection (e)(8) (notice of compelled disclosures) because requiring individual notice of legally compelled disclosure poses an impossible administrative burden and could alert subjects of counterterrorism, law enforcement, or intelligence investigations to the previously unknown fact of those investigations.

(11) From subsection (e)(12) (public notice of matching activity) because, to the extent such activities are not otherwise excluded from the matching requirements of the Privacy Act, publishing advance notice in the Federal Register would frustrate the ability of intelligence analysts to act quickly in furtherance of analytical efforts.

(12) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records and for assessing fees) because the system is exempt from the subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the
records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject’s access request.

(13) From subsection (g) (civil remedies) to the extent that the civil remedies relate to provisions of 5 U.S.C. 552a from which this rule exempts the system.

32 CFR Section 1701.24: Exemption of Office of the Director of National Intelligence (ODNI) systems of records.
(a) The ODNI exempts the following systems of records from the requirements of subsections (c)(3); (d)(1),(2),(3) and (4); (e)(1); (e)(4)(G),(H),(I); and (f) of the Privacy Act to the extent that information in the system is subject to exemption pursuant subsections (k)(1), (k)(2) or (k)(5) of the Act as noted in the individual systems notices:
(1) Manuscript, Presentation and Resume Review Records (ODNI-01).
(2) Executive Secretary Action Management System Records (ODNI-02).
(3) Public Affairs Office Records (ODNI-03).
(4) Office of Legislative Affairs Records (ODNI-04).
(5) ODNI Guest Speaker Records (ODNI-05).
(6) Office of General Counsel Records (ODNI-06).
(7) Analytic Resources Catalog (ODNI-07).
(8) Intelligence Community Customer Registry (ODNI-09).
(9) EEO and Diversity Office Records (ODNI-10).
(11) IC Security Clearance and Access Approval Repository (ODNI-12).
(13) Civil Liberties and Privacy Office Complaint Records (ODNI-14).
(b) Exemption of records in theses systems from any or all of the enumerated requirements may be necessary for the following reasons:
(1) From subsection (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an intelligence or investigative interest on the part of the ODNI or recipient agency and could result in release of properly classified national security or foreign policy information.
(2) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because affording access and amendment rights could alert the record subject to the investigative interest of intelligence or law enforcement agencies or compromise sensitive information classified in the interest of national security. In the absence of a national security basis for exemption, records in this system may be exempted from access and amendment to the extent necessary to honor promises of confidentiality to persons providing information concerning a candidate for position. Inability to maintain such confidentiality would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.
(3) From subsection (e)(1) (maintain only relevant and necessary records) because it is not always possible to establish relevance and necessity before all
information is considered and evaluated in relation to an intelligence concern. In the absence of a national security basis for exemption under subsection (k)(1), records in this system may be exempted from the relevance requirement pursuant to subsection (k)(5) because it is not possible to determine in advance what exact information may assist in determining the qualifications and suitability of a candidate for position. Seemingly irrelevant details, when combined with other data, can provide a useful composite for determining whether a candidate should be appointed.

(4) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment, and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the ODNI has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records.

(5) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information, intelligence sources and methods, and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement, ODNI identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in its systems of records.

(6) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees) because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the ODNI has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the ODNI may determine it appropriate to satisfy a record subject's access request.

[75 FR 57166, Sept. 20, 2010]
SUBPART C—Routine Uses Applicable to More Than One ODNI System of Records

32 CFR Section 1701.30: Policy and applicability.
(a) ODNI proposes the following general routine uses to foster simplicity and economy and to avoid redundancy or error by duplication in multiple ODNI systems of records and in systems of records established hereafter by ODNI or by one of its components.
(b) These general routine uses may apply to every Privacy Act system of records maintained by ODNI and its components, unless specifically stated otherwise in the System of Records Notice for a particular system. Additional general routine uses may be identified as notices of systems of records are published.
(c) Routine uses specific to a particular System of Records are identified in the System of Records Notice for that system.

32 CFR Section 1701.31: General routine uses.
(a) Except as noted on Standard Forms 85 and 86 and supplemental forms thereto (questionnaires for employment in, respectively, “non-sensitive” and “national security” positions within the Federal government), a record that on its face or in conjunction with other information indicates or relates to a violation or potential violation of law, whether civil, criminal, administrative or regulatory in nature, and whether arising by general statute, particular program statute, regulation, rule or order issued pursuant thereto, may be disclosed as a routine use to an appropriate federal, state, territorial, tribal, local law enforcement authority, foreign government or international law enforcement authority, or to an appropriate regulatory body charged with investigating, enforcing, or prosecuting such violations.
(b) A record from a system of records maintained by the ODNI may be disclosed as a routine use, subject to appropriate protections for further disclosure, in the course of presenting information or evidence to a magistrate, special master, administrative law judge, or to the presiding official of an administrative board, panel or other administrative body.
(c) A record from a system of records maintained by the ODNI may be disclosed as a routine use to representatives of the Department of Justice or any other entity responsible for representing the interests of the ODNI in connection with potential or actual civil, criminal, administrative, judicial or legislative proceedings or hearings, for the purpose of representing or providing advice to: The ODNI; any staff of the ODNI in his or her official capacity; any staff of the ODNI in his or her individual capacity where the staff has submitted a request for representation by the United States or for reimbursement of expenses associated with retaining counsel; or the United States or another Federal agency, when the United States or the agency is a party to such proceeding and the record is relevant and necessary to such proceeding.
(d) A record from a system of records maintained by the ODNI may be disclosed as a routine use in a proceeding before a court or adjudicative body when any of the following is a party to litigation or has an interest in such litigation, and the
ODNI, Office of General Counsel, determines that use of such records is relevant and necessary to the litigation: The ODNI; any staff of the ODNI in his or her official capacity; any staff of the ODNI in his or her individual capacity where the Department of Justice has agreed to represent the staff or has agreed to provide counsel at government expense; or the United States or another Federal agency, where the ODNI, Office of General Counsel, determines that litigation is likely to affect the ODNI.

(e) A record from a system of records maintained by the ODNI may be disclosed as a routine use to representatives of the Department of Justice and other U.S. Government entities, to the extent necessary to obtain advice on any matter within the official responsibilities of such representatives and the responsibilities of the ODNI.

(f) A record from a system of records maintained by the ODNI may be disclosed as a routine use to a Federal, state or local agency or other appropriate entities or individuals from which/whom information may be sought relevant to: A decision concerning the hiring or retention of an employee or other personnel action; the issuing or retention of a security clearance or special access, contract, grant, license, or other benefit; or the conduct of an authorized investigation or inquiry, to the extent necessary to identify the individual, inform the source of the nature and purpose of the inquiry, and identify the type of information requested.

(g) A record from a system of records maintained by the ODNI may be disclosed as a routine use to any Federal, state, local, tribal or other public authority, or to a legitimate agency of a foreign government or international authority to the extent the record is relevant and necessary to the other entity's decision regarding the hiring or retention of an employee or other personnel action; the issuing or retention of a security clearance or special access, contract, grant, license, or other benefit; or the conduct of an authorized inquiry or investigation.

(h) A record from a system of records maintained by the ODNI may be disclosed as a routine use to a Member of Congress or Congressional staffer in response to an inquiry from that Member of Congress or Congressional staffer made at the written request of the individual who is the subject of the record.

(i) A record from a system of records maintained by the ODNI may be disclosed to the Office of Management and Budget in connection with the review of private relief legislation, as set forth in Office of Management and Budget Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in the Circular.

(j) A record from a system of records maintained by the ODNI may be disclosed as a routine use to any agency, organization, or individual for authorized audit operations, and for meeting related reporting requirements, including disclosure to the National Archives and Records Administration for records management inspections and such other purposes conducted under the authority of 44 U.S.C. 2904 and 2906, or successor provisions.

(k) A record from a system of records maintained by the ODNI may be disclosed as a routine use to individual members or staff of Congressional intelligence oversight committees in connection with the exercise of the committees' oversight and legislative functions.
(l) A record from a system of records maintained by the ODNI may be disclosed as a routine use pursuant to Executive Order to the President's Foreign Intelligence Advisory Board, the President's Intelligence Oversight Board, to any successor organizations, and to any intelligence oversight entity established by the President, when the Office of the General Counsel or the Office of the Inspector General determines that disclosure will assist such entities in performing their oversight functions and that such disclosure is otherwise lawful.

(m) A record from a system of records maintained by the ODNI may be disclosed as a routine use to contractors, grantees, experts, consultants, or others when access to the record is necessary to perform the function or service for which they have been engaged by the ODNI.

(n) A record from a system of records maintained by the ODNI may be disclosed as a routine use to a former staff of the ODNI for the purposes of responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority or facilitating communications with a former staff of the ODNI that may be necessary for personnel-related or other official purposes when the ODNI requires information or consultation assistance, or both, from the former staff regarding a matter within that person's former area of responsibility.

(o) A record from a system of records maintained by the ODNI may be disclosed as a routine use to legitimate foreign, international or multinational security, investigatory, law enforcement or administrative authorities in order to comply with requirements imposed by, or to claim rights conferred in, formal agreements and arrangements to include those regulating the stationing and status in foreign countries of Department of Defense military and civilian personnel.

(p) A record from a system of records maintained by the ODNI may be disclosed as a routine use to any Federal agency when documents or other information obtained from that agency are used in compiling the record and the record is relevant to the official responsibilities of that agency, provided that disclosure of the recompiled or enhanced record to the source agency is otherwise authorized and lawful.

(q) A record from a system of records maintained by the ODNI may be disclosed as a routine use to appropriate agencies, entities, and persons when: The security or confidentiality of information in the system of records has or may have been compromised; and the compromise may result in economic or material harm to individuals (e.g., identity theft or fraud), or harm to the security or integrity of the affected information or information technology systems or programs (whether or not belonging to the ODNI) that rely upon the compromised information; and disclosure is necessary to enable ODNI to address the cause(s) of the compromise and to prevent, minimize, or remedy potential harm resulting from the compromise.

(r) A record from a system of records maintained by the ODNI may be disclosed as a routine use to a Federal, state, local, tribal, territorial, foreign, or multinational agency or entity or to any other appropriate entity or individual for any of the following purposes: to provide notification of a serious terrorist threat
for the purpose of guarding against or responding to such threat; to assist in coordination of terrorist threat awareness, assessment, analysis, or response; or to assist the recipient in performing authorized responsibilities relating to terrorism or counterterrorism.

(s) A record from a system of records maintained by the ODNI may be disclosed as a routine use for the purpose of conducting or supporting authorized counterintelligence activities as defined by section 401a(3) of the National Security Act of 1947, as amended, to elements of the Intelligence Community, as defined by section 401a(4) of the National Security Act of 1947, as amended; to the head of any Federal agency or department; to selected counterintelligence officers within the Federal government.

(t) A record from a system of records maintained by the ODNI may be disclosed as a routine use to a Federal, state, local, tribal, territorial, foreign, or multinational government agency or entity, or to other authorized entities or individuals, but only if such disclosure is undertaken in furtherance of responsibilities conferred by, and in a manner consistent with, the National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002, as amended; Executive Order 12333 or any successor order together with its implementing procedures approved by the Attorney General; and other provisions of law, Executive Order or directive relating to national intelligence or otherwise applicable to the ODNI. This routine use is not intended to supplant the other routine uses published by the ODNI.
32 CFR PART 1702—PROCEDURES GOVERNING THE ACCEPTANCE OF SERVICE OF PROCESS

- 1702.1: Scope and purpose.
- 1702.2: Definitions.
- 1702.3: Procedures governing acceptance of service of process.
- 1702.4: Notification to Office of General Counsel.
- 1702.5: Interpretation.

Authority:

Source:
74 FR 11479, Mar. 18, 2009, unless otherwise noted.

32 CFR Section 1702.1: Scope and purpose.
This part sets forth the ODNI policy concerning service of process upon the ODNI and ODNI employees in their official, individual or combined official and individual capacities. This part is intended to ensure the orderly execution of ODNI affairs and is not intended to impede the legal process.

32 CFR Section 1702.2: Definitions.
For purposes of this part the following terms have the following meanings:

DNI.

The Director of National Intelligence.

General Counsel.

The ODNI's General Counsel, Acting General Counsel or Deputy General Counsel.

ODNI.

The Office of the Director of National Intelligence and all of its components, including, but not limited to, the National Counterintelligence Executive, the National Counterterrorism Center, the National Counterproliferation Center, the
Program Manager for the Information Sharing Environment, and all national intelligence centers and program managers the DNI may establish.

**ODNI Employee.**

Any current or former employee, contractor, independent contractor, assignee or detailee to the ODNI.

**OGC.**

The Office of the General Counsel of the ODNI.

**Process.**

A summons, complaint, subpoena or other document properly issued by or under the authority of, a federal, state, local or other government entity of competent jurisdiction.

32 CFR Section 1702.3: Procedures governing acceptance of service of process.

(a) Service of process upon the ODNI or an ODNI employee in the employee's official capacity.

(1) Personal service. Unless otherwise expressly authorized by the General Counsel, personal service of process upon the ODNI or an ODNI employee in the employee's official capacity, may be accepted only by an OGC attorney at ODNI Headquarters. The OGC attorney shall write or stamp “Service Accepted In Official Capacity Only” on the return of service form.

(2) Mail service. Where service of process by registered or certified mail is authorized by law, only an OGC attorney may accept such service of process upon the ODNI or an ODNI employee in the employee's official capacity, unless otherwise expressly authorized by the General Counsel. The OGC attorney shall write or stamp “Service Accepted In Official Capacity Only,” on the waiver of personal service form. Service of process by mail must be addressed to the Office of the Director of National Intelligence, Office of General Counsel, Washington, DC 20511, and the envelope must be conspicuously marked “Service of Process.”

(b) Service of process upon an ODNI employee solely in the employee's individual capacity.

(1) Generally. ODNI employees will not be required to accept service of process in their purely individual capacity on ODNI facilities or premises.

(2) Personal Service. Subject to the sole discretion of the General Counsel, process servers generally will not be allowed to enter ODNI facilities or premises for the purpose of serving process upon an ODNI employee solely in the employee's individual capacity.
Except for the DNI, the Principal Deputy Director of National Intelligence, and the Director of the Intelligence Staff, the OGC is not authorized to accept service of process on behalf of any ODNI employee in the employee's individual capacity. (3) Mail Service.
Unless otherwise expressly authorized by the General Counsel, ODNI employees are not authorized to accept or forward mailed service of process directed to another ODNI employee in that employee's individual capacity. Any such process will be returned to the sender via appropriate postal channels.
(c) Service of Process Upon an ODNI employee in a combined official and individual capacity. Unless otherwise expressly authorized by the General Counsel, service of process, in person or by mail, upon an ODNI employee in the employee's combined official and individual capacity, may be accepted only for the ODNI employee in the employee's official capacity by an OGC attorney at ODNI Headquarters. The OGC attorney shall write or stamp, “Service Accepted In Official Capacity Only,” on the return of service form.
(d) Acceptance of service of process shall not constitute an admission or waiver with respect to jurisdiction, propriety of service, improper venue or any other defense in law or equity available under the laws or rules applicable to the service of process.

32 CFR Section 1702.4: Notification to Office of General Counsel.
An ODNI employee who receives or has reason to expect to receive, service of process in an official, individual or combined individual and official capacity in a matter that may involve testimony or the furnishing of documents that could reasonably be expected to involve ODNI interests, shall promptly notify the OGC ((703) 275-2527) prior to responding to the service in any manner, and if possible, before accepting service.

32 CFR Section 1702.5: Interpretation.
Any questions concerning interpretation of this regulation shall be referred to the Office of General Counsel for resolution.
32 CFR PART 1703—PRODUCTION OF ODNI INFORMATION OR MATERIAL IN PROCEEDINGS BEFORE FEDERAL, STATE, LOCAL OR OTHER GOVERNMENT ENTITY OF COMPETENT JURISDICTION

➤ 1703.1: Scope and purpose.
➤ 1703.2: Definitions.
➤ 1703.3: General.
➤ 1703.4: Procedure for production.
➤ 1703.5: Interpretation.

Authority:

Source:
74 FR 11480, Mar. 18, 2009, unless otherwise noted.

32 CFR Section 1703.1: Scope and purpose.
This part sets forth the policy and procedures with respect to the production or disclosure of material contained in the files of the ODNI, information relating to or based upon material contained in the files of the ODNI, and information acquired by any person while such person was an employee of the ODNI as part of the performance of that person’s official duties or because of that person’s association with the ODNI.

32 CFR Section 1703.2: Definitions.
The following definitions apply to this part:

Defenses:
Any and all legal defenses, privileges or objections available to the ODNI in response to a demand.

Demand:
(1) Any subpoena, order or other legal summons issued by a federal, state, local or other government entity of competent jurisdiction with the authority to require a response on a particular matter or a request for appearance of an individual where a demand could issue.
(2) Any request for production or disclosure which may result in the issuance of a subpoena, order, or other legal process to compel production or disclosure.

DNI:
The Director of National Intelligence.

General Counsel:
The ODNI's General Counsel, Acting General Counsel or Deputy General Counsel.

ODNI:
The Office of the Director of National Intelligence and all of its components, including, but not limited to, the Office of the National Counterintelligence Executive, the National Counterterrorism Center, the National Counterproliferation Center, the Program Manager for the Information Sharing Environment, and all national intelligence centers and program managers the DNI may establish.

ODNI Employee:
Any current or former employee, contractor, independent contractor, assignee or detailee to the ODNI.

ODNI Information or Material:
Information or material that is contained in ODNI files, related to or based upon material contained in ODNI files or acquired by any ODNI employee as part of that employee's official duties or because of that employee's association with the ODNI.

OGC:
The Office of the General Counsel of the ODNI.
OGC Attorney:

Any attorney in the OGC.

Proceeding:

Any matter before a court of law, administrative law judge, administrative tribunal or commission or other body that conducts legal or administrative proceedings, and includes all phases of the proceeding.

Production or Produce:

The disclosure of ODNI information or material in response to a demand.

32 CFR Section 1703.3: General.
(a) No ODNI employee shall respond to a demand for ODNI information or material without prior authorization as set forth in this part.
(b) This part is intended only to provide procedures for responding to demands for production of documents or information, and does not create any right or benefit, substantive or procedural, enforceable by any party against the United States.

32 CFR Section 1703.4: Procedure for production.
(a) Whenever a demand is made for ODNI information or material, the employee who received the demand shall immediately notify OGC ((703) 275-2527). The OGC and the ODNI employee shall then follow the procedures set forth in this section.
(b) The OGC may assert any and all defenses before any search for potentially responsive ODNI information or material begins. Further, in its sole discretion the ODNI may decline to begin a search for potentially responsive ODNI information or material until a final and non-appealable disposition of any or all of the asserted defenses is made by the federal, state, local or government entity of competent jurisdiction. When the OGC determines that it is appropriate to search for potentially responsive ODNI information and material, the OGC will forward the demand to the appropriate ODNI offices or entities with responsibility for the ODNI information or material sought in the demand. Those ODNI offices or entities shall then search for and provide to the OGC all potentially responsive ODNI information and material. The OGC may then assert any and all defenses to the production of what it determines is responsive ODNI information or material.
(c) In reaching a decision on whether to produce responsive ODNI information or material, or to object to the demand, the OGC shall consider whether:
(1) Any relevant privileges are applicable;
(2) The applicable rules of discovery or procedure require production;
(3) Production would violate a statute, regulation, executive order or other provision of law;
(4) Production would violate a non-disclosure agreement;
(5) Production would be inconsistent with the DNI's responsibility to protect intelligence sources and methods, or reveal classified information or state secrets;
(6) Production would violate a specific ODNI policy issuance or instruction; and
(7) Production would unduly interfere with the orderly conduct of ODNI functions.
(d) If oral or written testimony is sought by a demand in a case or matter in which the ODNI is not a party, a reasonably detailed description of the testimony sought in the form of an affidavit, or a written statement if that is not feasible, by the party seeking the testimony or its attorney must be furnished to the OGC.
(e) The OGC shall notify the appropriate employees of all decisions regarding responses to demands and provide advice and counsel for the implementation of the decisions.
(f) If response to a demand is required before a decision is made whether to provide responsive ODNI information or material, an OGC attorney will request that a Department of Justice attorney appear with the ODNI employee upon whom that demand has been made before the court or other competent authority and provide it with a copy of this regulation and inform the court or other authority as to the status of the demand. The court will be requested to stay the demand pending resolution by the ODNI. If the request for a stay is denied or there is a ruling that the demand must be complied with irrespective of instructions rendered in accordance with this Part, the employee upon whom the demand was made shall, if directed to do so by the General Counsel or its designee, respectfully decline to comply with the demand under the authority of United States ex rel. Touhy v. Ragen, 340 U.S. 462 (1951), and this regulation.
(g) ODNI officials may delegate in writing any authority given to them in this part to subordinate officials.
(h) Any individual or entity not an ODNI employee as defined in this part who receives a demand for the production or disclosure of ODNI information or material acquired because of that person's or entity's association with the ODNI should notify the OGC ((703) 275-2527) for guidance and assistance. In such cases the provisions of this regulation shall be applicable.

32 CFR Section 1703.5: Interpretation.
Any questions concerning interpretation of this Regulation shall be referred to the OGC for resolution.
Subpart A—General
  o 1800.1: Authority and purpose.
  o 1800.2: Definitions.
  o 1800.3: Contact for general information and requests.
  o 1800.4: Suggestions and complaints.
Subpart B—Filing of FOIA Requests
  o 1800.11: Preliminary information.
  o 1800.12: Requirements as to form and content.
  o 1800.13: Fees for record services.
  o 1800.14: Fee estimates (pre-request option).
Subpart C—NACIC Action on FOIA Requests
  o 1800.21: Processing of requests for records.
  o 1800.22: Action and determination(s) by originator(s) or any interested party.
  o 1800.23: Payment of fees, notification of decision, and right of appeal.
Subpart D—Additional Administrative Matters
  o 1800.31: Procedures for business information.
  o 1800.32: Procedures for information concerning other persons.
  o 1800.33: Allocation of resources; agreed extensions of time.
  o 1800.34: Requests for expedited processing.
Subpart E—NACIC Action on FOIA Administrative Appeals
  o 1800.41: Appeal authority.
  o 1800.42: Right of appeal and appeal procedures.
  o 1800.43: Determination(s) by Office Chief(s).
  o 1800.44: Action by appeals authority.
  o 1800.45: Notification of decision and right of judicial review.

Authority:
5 U.S.C. 552.
Source:
64 FR 49879, Sept. 14, 1999, unless otherwise noted.
SUBPART A—General
32 CFR Section 1800.1: Authority and purpose.
This part is issued under the authority of and in order to implement the Freedom of Information Act (FOIA), as amended (5 U.S.C. 552); and section 102 of the National Security Act of 1947, as amended (50 U.S.C. 403). It prescribes procedures for:
(a) Requesting information on available NACIC records, or NACIC administration of the FOIA, or estimates of fees that may become due as a result of a request;
(b) Requesting records pursuant to the FOIA; and
(c) Filing an administrative appeal of an initial adverse decision under the FOIA.

32 CFR Section 1800.2: Definitions.
For purposes of this part, the following terms have the meanings indicated:

NACIC

means the United States National Counterintelligence Center acting through the NACIC Information and Privacy Coordinator;

Days

means calendar days when NACIC is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this part if responding by U.S. domestic mail; otherwise ten (10) days may be added if responding by international mail;

Control

means ownership or the authority of NACIC pursuant to federal statute or privilege to regulate official or public access to records;

Coordinator

means the NACIC Information and Privacy Coordinator who serves as the NACIC manager of the information review and release program instituted under the Freedom of Information Act;

Direct-costs

means those expenditures which an agency actually incurs in the processing of a FOIA request; it does not include overhead factors such as space; it does include:
(1) Pages means paper copies of standard office size or the dollar value equivalent in other media;
(2) Reproduction means generation of a copy of a requested record in a form appropriate for release;
(3) Review means all time expended in examining a record to determine whether any portion must be withheld pursuant to law and in effecting any required deletions but excludes personnel hours expended in resolving general legal or policy issues; it also means personnel hours of professional time;
(4) Search means all time expended in looking for and retrieving material that may be responsive to a request utilizing available paper and electronic indices and finding aids; it also means personnel hours of professional time or the dollar value equivalent in computer searches;

Expression of interest

means a written communication submitted by a member of the public requesting information on or concerning the FOIA program and/or the availability of documents from NACIC;

Federal agency

means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

Fees

means those direct costs which may be assessed a requester considering the categories established by the FOIA; requesters should submit information to assist NACIC in determining the proper fee category and NACIC may draw reasonable inferences from the identity and activities of the requester in making such determinations; the fee categories include:
(1) Commercial means a request in which the disclosure sought is primarily in the commercial interest of the requester and which furthers such commercial, trade, income or profit interests;
(2) Non-commercial educational or scientific institution means a request from an accredited United States educational institution at any academic level or institution engaged in research concerning the social, biological, or physical sciences or an instructor or researcher or member of such institutions; it also means that the information will be used in a specific scholarly
or analytical work, will contribute to the advancement of public knowledge, and will be disseminated to the general public;

(3) Representative of the news media means a request from an individual actively gathering news for an entity that is organized and operated to publish and broadcast news to the American public and pursuant to their news dissemination function and not their commercial interests;

the term news means information which concerns current events, would be of current interest to the general public, would enhance the public understanding of the operations or activities of the U.S. Government, and is in fact disseminated to a significant element of the public at minimal cost; freelance journalists are included in this definition if they can demonstrate a solid basis for expecting publication through such an organization, even though not actually employed by it; a publication contract or prior publication record is relevant to such status;

(4) All other means a request from an individual not within categories (h)(1), (2), or (3) of this section;

Freedom of Information Act or “FOIA” means the statutes as codified at 5 U.S.C. 552;

Interested party means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of NACIC, has a subject matter or physical interest in the documents or information at issue;

Originator means the U.S. Government official who originated the document at issue or successor in office or such official who has been delegated release or declassification authority pursuant to law;

Potential requester means a person, organization, or other entity who submits an expression of interest;

Reasonably described records
means a description of a document (record) by unique identification number or descriptive terms which permit a NACIC employee to locate documents with reasonable effort given existing indices and finding aids;

Records or agency records

means all documents, irrespective of physical or electronic form, made or received by NACIC in pursuance of federal law or in connection with the transaction of public business and appropriate for preservation by NACIC as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of NACIC or because of the informational value of the data contained therein; it does not include:

(1) Books, newspapers, magazines, journals, magnetic or printed transcripts of electronic broadcasts, or similar public sector materials acquired generally and/or maintained for library or reference purposes; to the extent that such materials are incorporated into any form of analysis or otherwise distributed or published by NACIC, they are fully subject to the disclosure provisions of the FOIA;

(2) Index, filing, or museum documents made or acquired and preserved solely for reference, indexing, filing, or exhibition purposes; and

(3) Routing and transmittal sheets and notes and filing or destruction notes which do not also include information, comment, or statements of substance;

Responsive records

means those documents (i.e., records) which NACIC has determined to be within the scope of a FOIA request.

32 CFR Section 1800.3: Contact for general information and requests.
For general information on this part, to inquire about the FOIA program at NACIC, or to file a FOIA request (or expression of interest), please direct your communication in writing to the Information and Privacy Coordinator, Executive Secretariat Office, National Counterintelligence Center, 3W01 NHB, Washington, DC 20505. Such inquiries will also be accepted by facsimile at (703)874-5844. For general information or status information on pending cases only, the telephone number is (703)874-4121. Collect calls cannot be accepted.

32 CFR Section 1800.4: Suggestions and complaints.
NACIC welcomes suggestions or complaints with regard to its administration of the Freedom of Information Act. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. NACIC will respond
to all substantive communications and take such actions as determined feasible and appropriate.
SUBPART B—Filing of FOIA Requests

32 CFR Section 1800.11: Preliminary information.
Members of the public shall address all communications to the NACIC Coordinator as specified at § 1800.03 and clearly delineate the communication as a request under the Freedom of Information Act and this regulation. NACIC employees receiving a communication in the nature of a FOIA request shall expeditiously forward same to the Coordinator. Requests and appeals on requests, referrals, or coordinations received from members of the public who owe outstanding fees for information services at this or other federal agencies will not be accepted and action on all pending requests shall be terminated in such circumstances.

32 CFR Section 1800.12: Requirements as to form and content.

(a) Required information.

No particular form is required. A request need only reasonably describe the records of interest. This means that documents must be described sufficiently to enable a professional employee familiar with the subject to locate the documents with a reasonable effort. Commonly this equates to a requirement that the documents must be locatable through the indexing of our various systems. Extremely broad or vague requests or requests requiring research do not satisfy this requirement.

(b) Additional information for fee determination.

In addition, a requester should provide sufficient personal identifying information to allow us to determine the appropriate fee category. A requester should also provide an agreement to pay all applicable fees or fees not to exceed a certain amount or request a fee waiver.

(c) Otherwise.

Communications which do not meet these requirements will be considered an expression of interest and NACIC will work with, and offer suggestions to, the potential requester in order to define a request properly.

32 CFR Section 1800.13: Fees for record services.

(a) In general.

Search, review, and reproduction fees will be charged in accordance with the provisions below relating to schedule, limitations, and category of requester. Applicable fees will be due even if our search locates no responsive records or some or all of the responsive records must be denied under one or more of the exemptions of the Freedom of Information Act.
(b) Fee waiver requests.

Records will be furnished without charge or at a reduced rate whenever NACIC determines:
(1) That, as a matter of administrative discretion, the interest of the United States Government would be served, or
(2) That it is in the public interest because it is likely to contribute significantly to the public understanding of the operations or activities of the United States Government and is not primarily in the commercial interest of the requester; NACIC shall consider the following factors when making this determination:
(i) Whether the subject of the request concerns the operations or activities of the United States Government; and, if so,
(ii) Whether the disclosure of the requested documents is likely to contribute to an understanding of United States Government operations or activities; and, if so,
(iii) Whether the disclosure of the requested documents will contribute to public understanding of United States Government operations or activities; and
(iv) Whether the disclosure of the requested documents is likely to contribute significantly to public understanding of United States Government operations and activities; and
(v) Whether the requester has a commercial interest that would be furthered by the requested disclosure; and, if so,
(vi) Whether the disclosure is primarily in the commercial interest of the requester.

(c) Fee waiver appeals.

Denials of requests for fee waivers or reductions may be appealed to the Director, NACIC via the Coordinator. A requester is encouraged to provide any explanation or argument as to how his or her request satisfies the statutory requirement set forth in paragraph (b) of this section.

(d) Time for fee waiver requests and appeals.

It is suggested that such requests and appeals be made and resolved prior to the initiation of processing and the incurring of costs. However, fee waiver requests will be accepted at any time prior to the release of documents or the completion of a case, and fee waiver appeals within forty-five (45) days of our initial decision subject to the following condition: if processing has been initiated, then the requester must agree to be responsible for costs in the event of an adverse administrative or judicial decision.

(e) Agreement to pay fees.

In order to protect requesters from large and/or unanticipated charges, NACIC will request specific commitment when it estimates that fees will exceed $100.00. NACIC will hold in abeyance for forty-five (45) days requests requiring such
agreement and will thereafter deem the request closed. This action, of course, would not prevent an individual from refiling his or her FOIA request with a fee commitment at a subsequent date.

(f) Deposits.

NACIC may require an advance deposit of up to 100 percent of the estimated fees when fees may exceed $250.00 and the requester has no history of payment, or when, for fees of any amount, there is evidence that the requester may not pay the fees which would be accrued by processing the request. NACIC will hold in abeyance for forty-five (45) days those requests where deposits have been requested.

(g) Schedule of fees

(1) In general.
The schedule of fees for services performed in responding to requests for records is established as follows:

(i) Personnel Search and Review
   Clerical/Technical_Quarter hour_$ 5.00_Professional/Supervisory_Quarter hour_10.00_Manager/Senior Professional_Quarter hour_18.00

(ii) Computer Search and Production
   Search (on-line)_Flat rate_10.00_Search (off-line)_Flat rate_30.00_Other activity_Per minute_10.00_Tapes (mainframe cassette)_Each_9.00_Tapes (mainframe cartridge)_Each_9.00_Tapes (mainframe reel)_Each_20.00_Tapes (PC 9mm)_Each_25.00_Diskette (3.5")_Each_4.00_CD (bulk recorded)_Each_10.00_CD (recordable)_Each_20.00_Telecommunications_Per minute_50_ Paper (mainframe printer)_Per page_.10_Paper (PC b&w laser printer)_Per page_.10_Paper (PC color printer)_Per page_1.00

(iii) Paper Production
   Photocopy (standard or legal)_Per page_.10_Microfiche_Per frame_.20_Pre-printed (if available)_Per 100 pages_5.00_Published (if available)_Per item_NTIS_

(2) Application of schedule.
Personnel search time includes time expended in either manual paper records searches, indices searches, review of computer search results for relevance, personal computer system searches, and various reproduction services. In any event where the actual cost to NACIC of a particular item is less than the above schedule (e.g., a large production run of a document resulted in a cost less than $5.00 per hundred pages), then the actual lesser cost will be charged.
(3) Other services.
For all other types of output, production, or reproduction (e.g., photographs, maps, or published reports), actual cost or amounts authorized by statute. Determinations of actual cost shall include the commercial cost of the media, the personnel time expended in making the item to be released, and an allocated cost of the equipment used in making the item, or, if the production is effected by a commercial service, then that charge shall be deemed the actual cost for purposes of this part.

(h) Limitations on collection of fees

(1) In general.
No fees will be charged if the cost of collecting the fee is equal to or greater than the fee itself. That cost includes the administrative costs to NACIC of billing, receiving, recording, and processing the fee for deposit to the Treasury Department and, as of the date of these regulations, is deemed to be $10.00.

(2) Requests for personal information.
No fees will be charged for requesters seeking records about themselves under the FOIA; such requests are processed in accordance with both the FOIA and the Privacy Act in order to ensure the maximum disclosure without charge.

(i) Fee categories.
There are four categories of FOIA requesters for fee purposes: “commercial use” requesters, “educational and non-commercial scientific institution” requesters, “representatives of the news media” requesters, and “all other” requesters. The categories are defined in §1800.2, and applicable fees, which are the same in two of the categories, will be assessed as follows:
(1) “Commercial use” requesters: Charges which recover the full direct costs of searching for, reviewing, and duplicating responsive records (if any);
(2) “Educational and non-commercial scientific institution” requesters as well as “representatives of the news media” requesters: Only charges for reproduction beyond the first 100 pages;
(3) “All other” requesters: Charges which recover the full direct cost of searching for and reproducing responsive records (if any) beyond the first 100 pages of reproduction and the first two hours of search time which will be furnished without charge.

(j) Associated requests.
A requester or associated requesters may not file a series of multiple requests, which are merely discrete subdivisions of the information actually sought for the purpose of avoiding or reducing applicable fees. In such instances, NACIC may aggregate the requests and charge the applicable fees.

32 CFR Section 1800.14: Fee estimates (pre-request option).
In order to avoid unanticipated or potentially large fees, a requester may submit a request for a fee estimate. Pursuant to the Electronic Freedom of Information Act Amendments of 1996, NACIC will endeavor within twenty (20) days to provide an accurate estimate, and, if a request is thereafter submitted, NACIC will not accrue or charge fees in excess of our estimate without the specific permission of the requester.
SUBPART C—NACIC Action On FOIA Requests

32 CFR Section 1800.21: Processing of requests for records.

(a) In general.

Requests meeting the requirements of §§ 1800.11 through 1800.13 shall be accepted as formal requests and processed under the Freedom of Information Act, 5 U.S.C. 552, and these regulations. Pursuant to the Electronic Freedom of Information Act Amendments of 1996, upon receipt, NACIC shall within twenty (20) days record each request, acknowledge receipt to the requester in writing, and thereafter effect the necessary taskings to the NACIC components reasonably believed to hold responsive records.

(b) Database of “officially released information.”

As an alternative to extensive tasking and as an accommodation to many requesters, NACIC maintains a database of “officially released information” which contains copies of documents released by NACIC. Searches of this database can be accomplished expeditiously. Moreover, requests that are specific and well-focused will often incur minimal, if any, costs. Requesters interested in this means of access should so indicate in their correspondence. Consistent with the mandate of the Electronic Freedom of Information Act Amendments of 1996, online electronic access to these records is available to the public. Detailed information regarding such access is available from the point of contact specified in § 1800.3.

(c) Effect of certain exemptions.

In processing a request, NACIC shall decline to confirm or deny the existence or nonexistence of any responsive records whenever the fact of their existence or nonexistence is itself classified under Executive Order 12958 and may jeopardize intelligence sources or methods protected pursuant to section 103(c)(6) of the National Security Act of 1947. In such circumstances, NACIC, in the form of a final written response, shall so inform the requester and advise of his or her right to an administrative appeal.

(d) Time for response.

Pursuant to the Electronic Freedom of Information Act Amendments of 1996, NACIC will utilize every effort to determine within the statutory guideline of twenty (20) days after receipt of an initial request whether to comply with such a request. However, should the volume of requests require that NACIC seek additional time from a requester pursuant to § 1800.33, NACIC will inform the requester in writing and further advise of his or her right to file an administrative appeal of any adverse determination.
32 CFR Section 1800.22: Action and determination(s) by originator(s) or any interested party.

(a) Initial action for access.

(1) NACIC components tasked pursuant to a FOIA request shall search all relevant record systems within their cognizance. They shall:
(i) Determine whether a record exists;
(ii) Determine whether and to what extent any FOIA exemptions apply;
(iii) Approve the disclosure of all non-exempt records or portions of records for which they are the originator; and
(iv) Forward to the Coordinator all records approved for release or necessary for coordination with or referral to another originator or interested party.

(2) In making these decisions, the NACIC component officers shall be guided by the applicable law as well as the procedures specified at § 1800.31 and § 1800.32 regarding confidential commercial information and personal information (about persons other than the requester).

(b) Referrals and coordinations.

As applicable and within twenty (20) days, pursuant to the Electronic Freedom of Information Act Amendments of 1996, of receipt by the Coordinator, any NACIC records containing information originated by other NACIC components shall be forwarded to those entities for action in accordance with paragraph (a) of this section and return. Records originated by other federal agencies or NACIC records containing other federal agency information shall be forwarded to such agencies within twenty (20) days of our completion of initial action in the case for action under their regulations and direct response to the requester (for other agency records) or return to NACIC (for NACIC records).

32 CFR Section 1800.23: Payment of fees, notification of decision, and right of appeal.

(a) Fees in general.

Fees collected under this part do not accrue to the National Counterintelligence Center and shall be deposited immediately to the general account of the United States Treasury.

(b) Notification of decision.

Upon completion of all required review and the receipt of accrued fees (or promise to pay such fees), NACIC will promptly inform the requester in writing of those records or portions of records which may be released and which must be denied. With respect to the former, NACIC will provide copies; with respect to the latter, NACIC shall explain the reasons for the denial, identify the person(s)
responsible for such decisions by name and title, and give notice of a right of administrative appeal.

(c) Availability of reading room.

As an alternative to receiving records by mail, a requester may arrange to inspect the records deemed releasable at a NACIC “reading room” in the metropolitan Washington, DC area. Access will be granted after applicable and accrued fees have been paid. Requests to review or browse documents in our database of “officially released records” will also be honored in this manner to the extent that paper copies or electronic copies in unclassified computer systems exist. All such requests shall be in writing and addressed pursuant to § 1800.3. The records will be available at such times as mutually agreed but not less than three (3) days from our receipt of a request. The requester will be responsible for reproduction charges for any copies of records desired.
SUBPART D—Additional Administrative Matters

(a) In general.

Business information obtained by NACIC by a submitter shall not be disclosed pursuant to a Freedom of Information Act request except in accordance with this section. For purposes of this section, the following definitions apply:

*Business information* means commercial or financial information in which a legal entity has a recognized property interest;

*Confidential commercial information* means such business information provided to the United States Government by a submitter which is reasonably believed to contain information exempt from release under exemption (b)(4) of the Freedom of Information Act, 5 U.S.C. 552, because disclosure could reasonably be expected to cause substantial competitive harm;

*Submitter* means any person or entity who provides confidential commercial information to the United States Government; it includes, but is not limited to, corporations, businesses (however organized), state governments, and foreign governments; and

(b) Designation of confidential commercial information.

A submitter of business information will use good-faith efforts to designate, by appropriate markings, either at the time of submission or at a reasonable time thereafter, any portions of its submission that it considers to be confidential commercial information and hence protected from required disclosure pursuant to exemption (b)(4). Such designations shall expire ten (10) years after the date of the submission unless the submitter requests, and provides justification for, a longer designation period.

(c) Process in event of FOIA request

(1) Notice to submitters.

NACIC shall provide a submitter with prompt written notice of receipt of a Freedom of Information Act request encompassing business information whenever:

(i) The submitter has in good faith designated the information as confidential commercial information, or
(ii) NACIC believes that disclosure of the information could reasonably be expected to cause substantial competitive harm, and
(iii) The information was submitted within the last ten (10) years unless the submitter requested and provided acceptable justification for a specific notice period of greater duration.

(2) Form of notice.
This notice shall either describe the exact nature of the confidential commercial information at issue or provide copies of the responsive records containing such information.

(3) Response by submitter.
(i) Within seven (7) days of the above notice, all claims of confidentiality by a submitter must be supported by a detailed statement of any objection to disclosure. Such statement shall:
(A) Specify that the information has not been disclosed to the public;
(B) Explain why the information is contended to be a trade secret or confidential commercial information;
(C) Explain how the information is capable of competitive damage if disclosed;
(D) State that the submitter will provide NACIC and the Department of Justice with such litigation defense as requested; and
(E) Be certified by an officer authorized to legally bind the corporation or similar entity.
(ii) It should be noted that information provided by a submitter pursuant to this provision may itself be subject to disclosure under the FOIA.

(4) Decision and notice of intent to disclose.
(i) NACIC shall consider carefully a submitter's objections and specific grounds for nondisclosure prior to its final determination. If NACIC decides to disclose a document over the objection of a submitter, NACIC shall provide the submitter a written notice which shall include:
(A) A statement of the reasons for which the submitter's disclosure objections were not sustained;
(B) A description of the information to be disclosed; and
(C) A specified disclosure date which is seven (7) days after the date of the instant notice.
(ii) When notice is given to a submitter under this section, NACIC shall also notify the requester and, if NACIC notifies a submitter that it intends to disclose information, then the requester shall be notified also and given the proposed date for disclosure.

(5) Notice of FOIA lawsuit.
If a requester initiates a civil action seeking to compel disclosure of information asserted to be within the scope of this section, NACIC shall promptly notify the submitter. The submitter, as specified above, shall provide such litigation assistance as required by NACIC and the Department of Justice.
(6) Exceptions to notice requirement.
The notice requirements of this section shall not apply if NACIC determines that:
(i) The information should not be disclosed in light of other FOIA exemptions;
(ii) The information has been published lawfully or has been officially made available to the public;
(iii) The disclosure of the information is otherwise required by law or federal regulation; or
(iv) The designation made by the submitter under this section appears frivolous, except that, in such a case, NACIC will, within a reasonable time prior to the specified disclosure date, give the submitter written notice of any final decision to disclose the information.

[64 FR 49879, Sept. 14, 1999; 64 FR 53769, Oct. 4, 1999]

32 CFR Section 1800.32: Procedures for information concerning other persons.

(a) In general.

Personal information concerning individuals other than the requester shall not be disclosed under the Freedom of Information Act if the proposed release would constitute a clearly unwarranted invasion of personal privacy. See 5 U.S.C. 552(b)(6). For purposes of this section, the following definitions apply:

**Personal information**
means any information about an individual that is not a matter of public record, or easily discernible to the public, or protected from disclosure because of the implications that arise from Government possession of such information.

**Public interest**
means the public interest in understanding the operations and activities of the United States Government and not simply any matter which might be of general interest to the requester or members of the public.

(b) Determination to be made.

In making the required determination under this section and pursuant to exemption (b)(6) of the FOIA, NACIC will balance the privacy interests that would be compromised by disclosure against the public interest in release of the requested information.

(c) Otherwise.

A requester seeking information on a third person is encouraged to provide a signed affidavit or declaration from the third person waiving all or some of their
privacy rights. However, all such waivers shall be narrowly construed and the Coordinator, in the exercise of his discretion and administrative authority, may seek clarification from the third party prior to any or all releases.

32 CFR Section 1800.33: Allocation of resources; agreed extensions of time.

(a) In general.

NACIC components shall devote such personnel and other resources to the responsibilities imposed by the Freedom of Information Act as may be appropriate and reasonable considering:
1. The totality of resources available to the component,
2. The business demands imposed on the component by the Director of NACIC or otherwise by law,
3. The information review and release demands imposed by the Congress or other governmental authority, and
4. The rights of all members of the public under the various information review and disclosure laws.

(b) Discharge of FOIA responsibilities.

Components shall exercise due diligence in their responsibilities under the FOIA and must allocate a reasonable level of resources to requests under the Act in a strictly “first-in, first-out” basis and utilizing two or more processing queues to ensure that smaller as well as larger (i.e., project) cases receive equitable attention. The Information and Privacy Coordinator is responsible for management of the NACIC-wide program defined by this part and for establishing priorities for cases consistent with established law. The Director, NACIC shall provide policy and resource direction as necessary and render decisions on administrative appeals.

(c) Requests for extension of time.

When NACIC is unable to meet the statutory time requirements of the FOIA, it will inform the requester that the request cannot be processed within the statutory time limits, provide an opportunity for the requester to limit the scope of the request so that it can be processed within the statutory time limits, or arrange with the requester an agreed upon time frame for processing the request, or determine that exceptional circumstances mandate additional time in accordance with the definition of “exceptional circumstances” per section 552(a)(6)(C) of the Freedom of Information Act, as amended, effective October 2, 1997. In such instances NACIC will, however, inform a requester of his or her right to decline our request and proceed with an administrative appeal or judicial review as appropriate.
32 CFR Section 1800.34: Requests for expedited processing.

(a) In general.

All requests will be handled in the order received on a strictly “first-in, first-out” basis. Exceptions to this section will only be made in accordance with the following procedures. In all circumstances, however, and consistent with established judicial precedent, requests more properly the scope of requests under the Federal Rules of Civil or Criminal Procedure (or other federal, state, or foreign judicial or quasi-judicial rules) will not be granted expedited processing under this or related (e.g., Privacy Act) provisions unless expressly ordered by a federal court of competent jurisdiction.

(b) Procedure.

Requests for expedited processing will be approved only when a compelling need is established to the satisfaction of NACIC. A requester may make such a request with a certification of “compelling need” and, within ten (10) days of receipt, NACIC will decide whether to grant expedited processing and will notify the requester of its decision. The certification shall set forth with specificity the relevant facts upon which the requester relies and it appears to NACIC that substantive records relevant to the stated needs may exist and be deemed releasable. A “compelling need” is deemed to exist:

(1) When the matter involves an imminent threat to the life or physical safety of an individual; or

(2) When the request is made by a person primarily engaged in disseminating information and the information is relevant to a subject of public urgency concerning an actual or alleged Federal government activity.
SUBPART E—NACIC Action On FOIA Administrative Appeals

32 CFR Section 1800.41: Appeal authority.

The Director, NACIC will make final NACIC decisions from appeals of initial adverse decisions under the Freedom of Information Act and such other information release decisions made under parts 1801, 1802, and 1803 of this chapter. Matters decided by the Director, NACIC will be deemed a final decision by NACIC.

32 CFR Section 1800.42: Right of appeal and appeal procedures.

(a) Right of Appeal.

A right of administrative appeal exists whenever access to any requested record or any portion thereof is denied, no records are located in response to a request, or a request for a fee waiver is denied. NACIC will apprise all requesters in writing of their right to appeal such decisions to the Director, NACIC through the Coordinator.

(b) Requirements as to time and form.

Appeals of decisions must be received by the Coordinator within forty-five (45) days of the date of NACIC's initial decision. NACIC may, for good cause and as a matter of administrative discretion, permit an additional thirty (30) days for the submission of an appeal. All appeals shall be in writing and addressed as specified in § 1800.3. All appeals must identify the documents or portions of documents at issue with specificity and may present such information, data, and argument in support as the requester may desire.

(c) Exceptions.

No appeal shall be accepted if the requester has outstanding fees for information services at this or another federal agency. In addition, no appeal shall be accepted if the information in question has been the subject of a review within the previous two (2) years or is the subject of pending litigation in the federal courts.

(d) Receipt, recording, and tasking.

NACIC shall promptly record each request received under this part, acknowledge receipt to the requester in writing, and thereafter effect the necessary taskings to the office(s) which originated or has an interest in the record(s) subject to the appeal.

(e) Time for response.

NACIC shall attempt to complete action on an appeal within twenty (20) days of the date of receipt. The volume of requests, however, may require that NACIC
request additional time from the requester pursuant to § 1800.33. In such event, NACIC will inform the requester of the right to judicial review.

32 CFR Section 1800.43: Determination(s) by Office Chief(s).
Each Office Chief in charge of an office which originated or has an interest in any of the records subject to the appeal, or designee, is a required party to any appeal; other interested parties may become involved through the request of the Coordinator when it is determined that some or all of the information is also within their official cognizance. These parties shall respond in writing to the Coordinator with a finding as to the exempt status of the information. This response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the parties and consistent with the information rights of members of the general public under the various information review and release laws.

32 CFR Section 1800.44: Action by appeals authority.

(a) Preparation of docket.

The Coordinator shall provide a summation memorandum for consideration of the Director, NACIC; the complete record of the request consisting of the request, the document(s) (sanitized and full text) at issue, and the findings of concerned Office Chiefs or designee(s).

(b) Decision by the Director, NACIC.

The Director, NACIC shall personally decide each case; no personal appearances shall be permitted without the express permission of the Director, NACIC.

32 CFR Section 1800.45: Notification of decision and right of judicial review.
The Coordinator shall promptly prepare and communicate the decision of the Director, NACIC to the requester. With respect to any decision to deny information, that correspondence shall state the reasons for the decision, identify the officer responsible, and include a notice of a right to judicial review.
32 CFR PART 1801—PUBLIC RIGHTS UNDER THE PRIVACY ACT OF 1974

➢ Subpart A—General
  o 1801.1: Authority and purpose.
  o 1801.2: Definitions.
  o 1801.3: Contact for general information and requests.
  o 1801.4: Suggestions and complaints.

➢ Subpart B—Filing Of Privacy Act Requests
  o 1801.11: Preliminary information.
  o 1801.12: Requirements as to form.
  o 1801.13: Requirements as to identification of requester.
  o 1801.14: Fees.

➢ Subpart C—Action On Privacy Act Requests
  o 1801.21: Processing requests for access to or amendment of records.
  o 1801.22: Action and determination(s) by originator(s) or any interested party.
  o 1801.23: Notification of decision and right of appeal.

➢ Subpart D—Additional Administrative Matters
  o 1801.31: Special procedures for medical and psychological records.
  o 1801.32: Requests for expedited processing.
  o 1801.33: Allocation of resources; agreed extensions of time.

➢ Subpart E—Action On Privacy Act Administrative Appeals
  o 1801.41: Appeal authority.
  o 1801.42: Right of appeal and appeal procedures.
  o 1801.43: Determination(s) by Office Chief(s).
  o 1801.44: Action by appeals authority.
  o 1801.45: Notification of decision and right of judicial review.

➢ Subpart F—Prohibitions
  o 1801.51: Limitations on disclosure.
  o 1801.52: Criminal penalties.

➢ Subpart G—Exemptions
  o 1801.63: Specific exemptions.

Authority:

Source:
64 FR 49884, Sept. 14, 1999, unless otherwise noted.
SUBPART A—General
32 CFR Section 1801.1: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement the Privacy Act of 1974 (5 U.S.C. 552a) and section 102 of the National Security Act of 1947, as amended (50 U.S.C. 403).

(b) Purpose in general.

This part prescribes procedures for a requester, as defined herein:
(1) To request notification of whether the National Counterintelligence Center (NACIC) maintains a record concerning them in any non-exempt portion of a system of records or any non-exempt system of records;
(2) To request a copy of all non-exempt records or portions of records;
(3) To request that any such record be amended or augmented; and
(4) To file an administrative appeal to any initial adverse determination to deny access to or amend a record.

(c) Other purposes.

This part also sets forth detailed limitations on how and to whom NACIC may disclose personal information and gives notice that certain actions by officers or employees of the United States Government or members of the public could constitute criminal offenses.

32 CFR Section 1801.2: Definitions.
For purposes of this part, the following terms have the meanings indicated:

NACIC

means the United States National Counterintelligence Center acting through the NACIC Information and Privacy Coordinator;

Days

means calendar days when NACIC is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;
means ownership or the authority of NACIC pursuant to federal statute or privilege to regulate official or public access to records;

Coordinator

means the NACIC Information and Privacy Coordinator who serves as the NACIC manager of the information review and release program instituted under the Privacy Act;

Federal agency

means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of NACIC, has a subject matter or physical interest in the documents or information at issue;

Maintain

means maintain, collect, use, or disseminate;

Originator

means the U.S. Government official who originated the document at issue or successor in office or such official who has been delegated release or declassification authority pursuant to law;

Privacy Act or PA

means the statute as codified at 5 U.S.C. 552a;

Record

means an item, collection, or grouping of information about an individual that is maintained by NACIC in a system of records;
Requester or individual

means a citizen of the United States or an alien lawfully admitted for permanent residence who is a living being and to whom a record might pertain;

Responsive record

means those documents (records) which NACIC has determined to be within the scope of a Privacy Act request;

Routine use

means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which the record is maintained;

System of records

means a group of any records under the control of NACIC from which records are retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to that individual.

32 CFR Section 1801.3: Contact for general information and requests.

For general information on this part, to inquire about the Privacy Act program at NACIC, or to file a Privacy Act request, please direct your communication in writing to the Information and Privacy Coordinator, Executive Secretariat Office, National Counterintelligence Center, 3W01 NHB, Washington, DC 20505. Requests with the required identification statement pursuant to § 1801.13 must be filed in original form by mail. Subsequent communications and any inquiries will be accepted by mail or facsimile at (703) 874-5844 or by telephone at (703) 874-4121. Collect calls cannot be accepted.

32 CFR Section 1801.4: Suggestions and complaints.

NACIC welcomes suggestions or complaints with regard to its administration of the Privacy Act. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. NACIC will respond to all substantive communications and take such actions as determined feasible and appropriate.
SUBPART B—Filing Of Privacy Act Requests
32 CFR Section 1801.11: Preliminary information.
Members of the public shall address all communications to the contact specified at § 1801.3 and clearly delineate the communication as a request under the Privacy Act and this regulation. Requests and administrative appeals on requests, referrals, and coordinations received from members of the public who owe outstanding fees for information services at this or other federal agencies will not be accepted and action on existing requests and appeals will be terminated in such circumstances.

32 CFR Section 1801.12: Requirements as to form.

(a) In general.

No particular form is required. All requests must contain the identification information required at § 1801.13.

(b) For access.

For requests seeking access, a requester should, to the extent possible, describe the nature of the record sought and the record system(s) in which it is thought to be included. Requesters may find assistance from information described in the Privacy Act Issuances Compilation which is published biennially by the Federal Register.

In lieu of this, a requester may simply describe why and under what circumstances it is believed that NACIC maintains responsive records; NACIC will undertake the appropriate searches.

(c) For amendment.

For requests seeking amendment, a requester should identify the particular record or portion subject to the request, state a justification for such amendment, and provide the desired amending language.

32 CFR Section 1801.13: Requirements as to identification of requester.

(a) In general.

Individuals seeking access to or amendment of records concerning themselves shall provide their full (legal) name, address, date and place of birth, and current citizenship status together with a statement that such information is true under penalty of perjury or a notarized statement swearing to or affirming identity. If NACIC determines that this information is not sufficient, NACIC may request additional or clarifying information.
(b) Requirement for aliens.

Only aliens lawfully admitted for permanent residence (PRAs) may file a request pursuant to the Privacy Act and this part. Such individuals shall provide, in addition to the information required under paragraph (a) of this section, their Alien Registration Number and the date that status was acquired.

(c) Requirement for representatives.

The parent or guardian of a minor individual, the guardian of an individual under judicial disability, or an attorney retained to represent an individual shall provide, in addition to establishing the identity of the minor or individual represented as required in paragraph (a) or (b) of this section, evidence of such representation by submission of a certified copy of the minor's birth certificate, court order, or representational agreement which establishes the relationship and the requester's identity.

(d) Procedure otherwise.

If a requester or representative fails to provide the information in paragraph (a), (b), or (c) of this section within forty-five (45) days of the date of our request, NACIC will deem the request closed. This action, of course, would not prevent an individual from refiling his or her Privacy Act request at a subsequent date with the required information.

32 CFR Section 1801.14: Fees.
No fees will be charged for any action under the authority of the Privacy Act, 5 U.S.C. 552a, irrespective of the fact that a request is or may be processed under the authority of both the Privacy Act and the Freedom of Information Act.
SUBPART C—Action On Privacy Act Requests

32 CFR Section 1801.21: Processing requests for access to or amendment of records.

(a) In general.

Requests meeting the requirements of § 1801.11 through § 1801.13 shall be processed under both the Freedom of Information Act, 5 U.S.C. 552, and the Privacy Act, 5 U.S.C. 552a, and the applicable regulations, unless the requester demands otherwise in writing. Such requests will be processed under both Acts regardless of whether the requester cites one Act in the request, both, or neither. This action is taken in order to ensure the maximum possible disclosure to the requester.

(b) Receipt, recording and tasking.

Upon receipt of a request meeting the requirements of §§ 1801.11 through 1801.13, NACIC shall within ten (10) days record each request, acknowledge receipt to the requester, and thereafter effect the necessary taskings to the office(s) reasonably believed to hold responsive records.

(c) Effect of certain exemptions.

In processing a request, NACIC shall decline to confirm or deny the existence or nonexistence of any responsive records whenever the fact of their existence or nonexistence is itself classified under Executive Order 12958 and that confirmation of the existence of a record may jeopardize intelligence sources and methods protected pursuant to section 103(c)(6) of the National Security Act of 1947. In such circumstances, NACIC, in the form of a final written response, shall so inform the requester and advise of his or her right to an administrative appeal.

(d) Time for response.

Although the Privacy Act does not mandate a time for response, our joint treatment of requests under both the Privacy Act and the FOIA means that the NACIC should provide a response within the FOIA statutory guideline of ten (10) days on initial requests and twenty (20) days on administrative appeals. However, the volume of requests may require that NACIC seek additional time from a requester pursuant to § 1801.33. In such event, NACIC will inform the requester in writing and further advise of his or her right to file an administrative appeal.

32 CFR Section 1801.22: Action and determination(s) by originator(s) or any interested party.

(a) Initial action for access.
NACIC offices tasked pursuant to a Privacy Act access request shall search all relevant record systems within their cognizance. They shall:
(1) Determine whether responsive records exist;
(2) Determine whether access must be denied in whole or part and on what legal basis under both Acts in each such case;
(3) Approve the disclosure of records for which they are the originator; and
(4) Forward to the Coordinator all records approved for release or necessary for coordination with or referral to another originator or interested party as well as the specific determinations with respect to denials (if any).

(b) Initial action for amendment.

NACIC offices tasked pursuant to a Privacy Act amendment request shall review the official records alleged to be inaccurate and the proposed amendment submitted by the requester. If they determine that NACIC’s records are not accurate, relevant, timely or complete, they shall promptly:
(1) Make the amendment as requested;
(2) Write to all other identified persons or agencies to whom the record has been disclosed (if an accounting of the disclosure was made) and inform of the amendment; and
(3) Inform the Coordinator of such decisions.

(c) Action otherwise on amendment request.

If the NACIC office records manager declines to make the requested amendment (or declines to make the requested amendment) but agrees to augment the official records, that manager shall promptly:
(1) Set forth the reasons for refusal; and
(2) Inform the Coordinator of such decision and the reasons therefore.

(d) Referrals and coordinations.

As applicable and within ten (10) days of receipt by the Coordinator, any NACIC records containing information originated by other NACIC offices shall be forwarded to those entities for action in accordance with paragraphs (a), (b), or (c) of this section and return. Records originated by other federal agencies or NACIC records containing other federal information shall be forwarded to such agencies within ten (10) days of our completion of initial action in the case for action under their regulations and direct response to the requester (for other NACIC records) or return to NACIC (for NACIC records).

(e) Effect of certain exemptions.

This section shall not be construed to allow access to systems of records exempted by the Director, NACIC pursuant to subsections (j) and (k) of the Privacy Act or where those exemptions require that NACIC can neither confirm nor deny the existence or nonexistence of responsive records.
32 CFR Section 1801.23: Notification of decision and right of appeal.
Within ten (10) days of receipt of responses to all initial taskings and subsequent coordinations (if any), and dispatch of referrals (if any), NACIC will provide disclosable records to the requester. If a determination has been made not to provide access to requested records (in light of specific exemptions) or that no records are found, NACIC shall so inform the requester, identify the denying official, and advise of the right to administrative appeal.
SUBPART D—Additional Administrative Matters

32 CFR Section 1801.31: Special procedures for medical and psychological records.

(a) In general.

When a request for access or amendment involves medical or psychological records and when the originator determines that such records are not exempt from disclosure, NACIC will, after consultation with the Director of Medical Services, CIA, determine:
(1) Which records may be sent directly to the requester and
(2) Which records should not be sent directly to the requester because of possible medical or psychological harm to the requester or another person.

(b) Procedure for records to be sent to physician.

In the event that NACIC determines, in accordance with paragraph (a)(2) of this section, that records should not be sent directly to the requester, NACIC will notify the requester in writing and advise that the records at issue can be made available only to a physician of the requester’s designation. Upon receipt of such designation, verification of the identity of the physician, and agreement by the physician:
(1) To review the documents with the requesting individual,
(2) To explain the meaning of the documents, and
(3) To offer counseling designed to temper any adverse reaction, NACIC will forward such records to the designated physician.

(c) Procedure if physician option not available.

If within sixty (60) days of paragraph (a)(2) of this section, the requester has failed to respond or designate a physician, or the physician fails to agree to the release conditions, NACIC will hold the documents in abeyance and advise the requester that this action may be construed as a technical denial. NACIC will also advise the requester of the responsible official and of his or her rights to administrative appeal and thereafter judicial review.

32 CFR Section 1801.32: Requests for expedited processing.
(a) All requests will be handled in the order received on a strictly “first-in, first-out” basis. Exceptions to this rule will only be made in circumstances that NACIC deems to be exceptional. In making this determination, NACIC shall consider and must decide in the affirmative on all of the following factors:
(1) That there is a genuine need for the records; and
(2) That the personal need is exceptional; and
(3) That there are no alternative forums for the records sought; and
(4) That it is reasonably believed that substantive records relevant to the stated needs may exist and be deemed releasable.
(b) In sum, requests shall be considered for expedited processing only when health, humanitarian, or due process considerations involving possible deprivation of life or liberty create circumstances of exceptional urgency and extraordinary need. In accordance with established judicial precedent, requests more properly the scope of requests under the Federal Rules of Civil or Criminal Procedure (or equivalent state rules) will not be granted expedited processing under this or related (e.g., Freedom of Information Act) provisions unless expressly ordered by a federal court of competent jurisdiction.

32 CFR Section 1801.33: Allocation of resources; agreed extensions of time.

(a) In general.

NACIC components shall devote such personnel and other resources to the responsibilities imposed by the Privacy Act as may be appropriate and reasonable considering:
(1) The totality of resources available to the component,
(2) The business demands imposed on the component by the Director, NACIC or otherwise by law,
(3) The information review and release demands imposed by the Congress or other governmental authority, and
(4) The rights of all members of the public under the various information review and disclosure laws.

(b) Discharge of Privacy Act responsibilities.

Offices shall exercise due diligence in their responsibilities under the Privacy Act and must allocate a reasonable level of resources to requests under the Act in a strictly “first-in, first-out” basis and utilizing two or more processing queues to ensure that smaller as well as larger (i.e., project) cases receive equitable attention. The Information and Privacy Coordinator is responsible for management of the NACIC-wide program defined by this part and for establishing priorities for cases consistent with established law. The Director, NACIC shall provide policy and resource direction as necessary and shall render decisions on administrative appeals.

(c) Requests for extension of time.

While the Privacy Act does not specify time requirements, our joint treatment of requests under the FOIA means that when NACIC is unable to meet the statutory time requirements of the FOIA, NACIC may request additional time from a requester. In such instances NACIC will inform a requester of his or her right to decline our request and proceed with an administrative appeal or judicial review as appropriate.
SUBPART E—Action On Privacy Act Administrative Appeals

32 CFR Section 1801.41: Appeal authority.
The Director, NACIC will make final NACIC decisions from appeals of initial adverse decisions under the Privacy Act and such other information release decisions made under 32 CFR parts 1800, 1802, and 1803 of this chapter. Matters decided by the Director, NACIC will be deemed a final decision by NACIC.

32 CFR Section 1801.42: Right of appeal and appeal procedures.

(a) Right of Appeal.

A right of administrative appeal exists whenever access to any requested record or any portion thereof is denied, no records are located in response to a request, or a request for amendment is denied. NACIC will apprise all requesters in writing of their right to appeal such decisions to the Director, NACIC through the Coordinator.

(b) Requirements as to time and form.

Appeals of decisions must be received by the Coordinator within forty-five (45) days of the date of NACIC's initial decision. NACIC may, for good cause and as a matter of administrative discretion, permit an additional thirty (30) days for the submission of an appeal. All appeals to the Director, NACIC shall be in writing and addressed as specified in § 1801.3. All appeals must identify the documents or portions of documents at issue with specificity, provide the desired amending language (if applicable), and may present such information, data, and argument in support as the requester may desire.

(c) Exceptions.

No appeal shall be accepted if the requester has outstanding fees for information services at this or another federal agency. In addition, no appeal shall be accepted if the information in question has been the subject of an administrative review within the previous two (2) years or is the subject of pending litigation in the federal courts.

(d) Receipt, recording, and tasking.

NACIC shall promptly record each administrative appeal, acknowledge receipt to the requester in writing, and thereafter effect the necessary taskings to the office chief in charge of the office(s) which originated or has an interest in the record(s) subject to the appeal.

32 CFR Section 1801.43: Determination(s) by Office Chiefs.
Each Office Chief in charge of an office which originated or has an interest in any of the records subject to the appeal, or designee, is a required party to any appeal;
other interested parties may become involved through the request of the Coordinator when it is determined that some or all of the information is also within their official cognizance. These parties shall respond in writing to the Coordinator with a finding as to the exempt or non-exempt status of the information including citations to the applicable exemption and/or their agreement or disagreement as to the requested amendment and the reasons therefore. Each response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the parties and consistent with the information rights of members of the general public under the various information review and release laws.

32 CFR Section 1801.44: Action by appeals authority.

(a) Preparation of docket.

The Coordinator shall provide a summation memorandum for consideration of the Director, NACIC; the complete record of the request consisting of the request, the document(s) (sanitized and full text) at issue, and the findings of any concerned office chiefs or designee(s).

(b) Decision by the Director, NACIC.

The Director, NACIC shall personally decide each case; no personal appearances shall be permitted without the express permission of the Director, NACIC.

32 CFR Section 1801.45: Notification of decision and right of judicial review.

(a) In general.

The Coordinator shall promptly prepare and communicate the decision of the Director, NACIC to the requester. With respect to any decision to deny information or deny amendment, that correspondence shall state the reasons for the decision, identify the officer responsible, and include a notice of the right to judicial review.

(b) For amendment requests.

With further respect to any decision to deny an amendment, that correspondence shall also inform the requester of the right to submit within forty-five (45) days a statement of his or her choice which shall be included in the official records of NACIC. In such cases, the applicable record system manager shall clearly note any portion of the official record which is disputed, append the requester's statement, and provide copies of the statement to previous recipients (if any are known) and to any future recipients when and if the disputed information is disseminated in accordance with a routine use.
SUBPART F—Prohibitions

32 CFR Section 1801.51: Limitations on disclosure.

No record which is within a system of records shall be disclosed by any means of communication to any individual or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be:

(a) To those officers and employees of NACIC which maintains the record who have a need for the record in the performance of their duties;
(b) Required under the Freedom of Information Act, 5 U.S.C. 552;
(c) For a routine use as defined in § 1801.02(m), as contained in the Privacy Act Issuances Compilation which is published biennially in the Federal Register, and as described in sections (a)(7) and (e)(4)(D) of the Act;
(d) To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of U.S.C. Title 13;
(e) To a recipient who has provided NACIC with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
(f) To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or designee to determine whether the record has such value;
(g) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of that agency or instrumentality has made a written request to NACIC specifying the particular information desired and the law enforcement activity for which the record is sought;
(h) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
(i) To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
(j) To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office; or
(k) To any agency, government instrumentality, or other person or entity pursuant to the order of a court of competent jurisdiction of the United States or constituent states.

32 CFR Section 1801.52: Criminal penalties.

(a) Unauthorized disclosure.

Criminal penalties may be imposed against any officer or employee of NACIC who, by virtue of employment, has possession of or access to NACIC records
which contain information identifiable with an individual, the disclosure of which is prohibited by the Privacy Act or by these rules, and who, knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive same.

(b) Unauthorized maintenance.

Criminal penalties may be imposed against any officer or employee of NACIC who willfully maintains a system of records without meeting the requirements of section (e)(4) of the Privacy Act, 5 U.S.C. 552a. The Coordinator and the Director of NACIC are authorized independently to conduct such surveys and inspect such records as necessary from time to time to ensure that these requirements are met.

(c) Unauthorized requests.

Criminal penalties may be imposed upon any person who knowingly and willfully requests or obtains any record concerning an individual from NACIC under false pretenses.
SUBPART G—Exemptions

32 CFR Section 1801.63: Specific exemptions.
Pursuant to authority granted in section (k) of the Privacy Act, the Director, NACIC has determined to exempt from section (d) of the Privacy Act those portions and only those portions of all systems of records maintained by NACIC that would consist of, pertain to, or otherwise reveal information that is:
(a) Classified pursuant to Executive Order 12958 (or successor or prior Order) and thus subject to the provisions of 5 U.S.C. 552(b)(1) and 5 U.S.C. 552a(k)(1);
(b) Investigatory in nature and compiled for law enforcement purposes, other than material within the scope of section (j)(2) of the Act; provided however, that if an individual is denied any right, privilege, or benefit to which they are otherwise eligible, as a result of the maintenance of such material, then such material shall be provided to that individual except to the extent that the disclosure would reveal the identity of a source who furnished the information to the United States Government under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;
(c) Maintained in connection with providing protective services to the President of the United States or other individuals pursuant to 18 U.S.C. 3056;
(d) Required by statute to be maintained and used solely as statistical records;
(e) Investigatory in nature and compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the United States Government under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;
(f) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or
(g) Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the United States Government under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality.
32 CFR PART 1802—CHALLENGES TO CLASSIFICATION OF DOCUMENTS BY AUTHORIZED HOLDERS PURSUANT TO SECTION 1.9 OF EXECUTIVE ORDER 12958

- Subpart A—General
  - 1802.1: Authority and purpose.
  - 1802.2: Definitions.
  - 1802.3: Contact for general information and requests.
  - 1802.4: Suggestions and complaints.

- Subpart B—Filing of Challenges
  - 1802.11: Prerequisites.
  - 1802.12: Requirements as to form.
  - 1802.13: Identification of material at issue.
  - 1802.14: Transmission.

- Subpart C—Action on Challenges
  - 1802.21: Receipt, recording, and tasking.
  - 1802.22: Challenges barred by res judicata.
  - 1802.23: Determination by originator(s) and/or any interested party.
  - 1802.24: Designation of authority to hear challenges.
  - 1802.25: Action on challenge.
  - 1802.26: Notification of decision and prohibition on adverse action.

- Subpart D—Right of Appeal
  - 1802.31: Right of Appeal.

Authority:
Executive Order 12958, 60 FR 19825, 3 CFR 1996 Comp., p. 333-356 (or successor Orders).

Source:
64 FR 49889, Sept. 14, 1999, unless otherwise noted.
SUBPART A—General
32 CFR Section 1802.1: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement § 1.9 of Executive Order (E.O.) 12958 and section 102 of the National Security Act of 1947.

(b) Purpose.

This part prescribes procedures for authorized holders of information classified under the various provisions of E.O. 12958, or predecessor Orders, to seek a review or otherwise challenge the classified status of information to further the interests of the United States Government. This part and § 1.9 of E.O. 12958 confer no rights upon members of the general public, or authorized holders acting in their personal capacity, both of whom shall continue to request reviews of classification under the mandatory declassification review provisions set forth at § 3.6 of E.O. 12958.

32 CFR Section 1802.2: Definitions.
For purposes of this part, the following terms have the meanings as indicated:

NACIC

means the United States National Counterintelligence Center acting through the NACIC Information and Privacy Coordinator;

Authorized holders

means any member of any United States executive department, military department, the Congress, or the judiciary (Article III) who holds a security clearance from or has been specifically authorized by NACIC to possess and use on official business classified information, or otherwise has Constitutional authority pursuant to their office;

Days

means calendar days when NACIC is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any requirement of this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

Challenge
means a request in the individual’s official, not personal, capacity and in furtherance of the interests of the United States;

**Control**

means ownership or the authority of NACIC pursuant to federal statute or privilege to regulate official or public access to records;

**Coordinator**

means the NACIC Information and Privacy Coordinator acting in the capacity of the Director of NACIC;

**Information**

means any knowledge that can be communicated or documentary material, regardless of its physical form, that is:
(1) Owned by, produced by or for, or under the control of the United States Government, and
(2) Lawfully and actually in the possession of an authorized holder and for which ownership and control has not been relinquished by NACIC;

**Interested party**

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of NACIC, has a subject matter or physical interest in the documents or information at issue;

**Originator**

means the NACIC officer who originated the information at issue, or successor in office, or a NACIC officer who has been delegated declassification authority for the information at issue in accordance with the provisions of this Order;

**This Order**

means Executive Order 12958 of April 17, 1995, or successor Orders.

32 CFR Section 1802.3: Contact for general information and requests.
For information on this part or to file a challenge under this part, please direct your inquiry to the Director, National Counterintelligence Center, Washington, DC 20505. The commercial (non-secure) telephone is (703) 874-4117; the classified (secure) telephone for voice and facsimile is (703) 874-5829.

32 CFR Section 1802.4: Suggestions and complaints.
NACIC welcomes suggestions or complaints with regard to its administration of the Executive Order. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. NACIC will respond to all substantive communications and take such actions as determined feasible and appropriate.
SUBPART B—Filing Of Challenges

32 CFR Section 1802.11: Prerequisites.
Prior to reliance on this part, authorized holders are required to first exhaust such established administrative procedures for the review of classified information. Further information on these procedures is available from the point of contact, § 1802.3.

32 CFR Section 1802.12: Requirements as to form.
The challenge shall include identification of the challenger by full name and title of position, verification of security clearance or other basis of authority, and an identification of the documents or portions of documents or information at issue. The challenge shall also, in detailed and factual terms, identify and describe the reasons why it is believed that the information is not protected by one or more of the § 1.5 provisions, that the release of the information would not cause damage to the national security, or that the information should be declassified due to the passage of time. The challenge must be properly classified; in this regard, until the challenge is decided, the authorized holder must treat the challenge, the information being challenged, and any related or explanatory information as classified at the same level as the current classification of the information in dispute.

32 CFR Section 1802.13: Identification of material at issue.
Authorized holders shall append the documents at issue and clearly mark those portions subject to the challenge. If information not in documentary form is in issue, the challenge shall state so clearly and present or otherwise refer with specificity to that information in the body of the challenge.

32 CFR Section 1802.14: Transmission.
Authorized holders must direct challenge requests to NACIC as specified in § 1802.3. The classified nature of the challenge, as well as the appended documents, require that the holder transmit same in full accordance with established security procedures. In general, registered U.S. mail is approved for SECRET, non-compartmented material; higher classifications require use of approved Top Secret facsimile machines or NACIC-approved couriers. Further information is available from NACIC as well as corporate or other federal agency security departments.
SUBPART C—Action On Challenges

32 CFR Section 1802.21: Receipt, recording, and tasking.
The Coordinator shall within ten (10) days record each challenge received under this part, acknowledge receipt to the authorized holder, and task the originator and other interested parties. Additional taskings, as required during the review process, shall be accomplished within five (5) days of notification.

32 CFR Section 1802.22: Challenges barred by res judicata.
The Coordinator shall respond on behalf of the Director, NACIC and deny any challenge where the information in question has been the subject of a classification review within the previous two (2) years or is the subject of pending litigation in the federal courts.

32 CFR Section 1802.23: Response by originator(s) and/or any interested party.

(a) In general.
The originator of the classified information (document) is a required party to any challenge; other interested parties may become involved through the request of the Director, NACIC or the originator when it is determined that some or all of the information is also within their official cognizance.

(b) Determination.
These parties shall respond in writing to the Director, NACIC with a mandatory unclassified finding, to the greatest extent possible, and an optional classified addendum. This finding shall agree to a declassification or, in specific and factual terms, explain the basis for continued classification including identification of the category of information, the harm to national security which could be expected to result from disclosure, and, if older than ten (10) years, the basis for the extension of classification time under §§ 1.6 and 3.4 of this Order. These parties shall also provide a statement as to whether or not there is any other statutory, common law, or Constitutional basis for withholding as required by § 6.1(c) of this Order.

(c) Time.
The determination(s) shall be provided on a first in, first out basis with respect to all challenges pending under this section and shall be accomplished expeditiously taking into account the requirements of the authorized holder as well as the business requirements of the originator including their responsibilities under the Freedom of Information Act, the Privacy Act, or the mandatory declassification review provisions of this Order.

32 CFR Section 1802.24: Designation of authority to hear challenges.
The Director, NACIC is the NACIC authority to hear and decide challenges under this part.

32 CFR Section 1802.25: Action on challenge.
Action by Coordinator. The Coordinator shall provide a summation memorandum for consideration of the Director, NACIC; the complete package consisting of the challenge, the information at issue, and the findings of the originator and interested parties shall also be provided. The Director, NACIC shall personally decide each case; no personal appearances shall be permitted without the express permission of the Director, NACIC.

32 CFR Section 1802.26: Notification of decision and prohibition on adverse action.
The Coordinator shall communicate the decision of NACIC to the authorized holder, the originator, and other interested parties within ten (10) days of the decision by the Coordinator. That correspondence shall include a notice that no adverse action or retribution can be taken in regard to the challenge and that an appeal of the decision may be made to the Interagency Security Classification Appeals Panel (ISCAP) established pursuant to § 5.4 of this Order.
SUBPART D—Right of Appeal
32 CFR Section 1802.31: Right of appeal.
A right of appeal is available to the ISCAP established pursuant to § 5.4 of this Order. Action by that body will be the subject of rules to be promulgated by the Information Security Oversight Office (ISOO).
32 CFR PART 1803—PUBLIC REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW OF CLASSIFIED INFORMATION PURSUANT TO SECTION 3.6 OF EXECUTIVE ORDER 12958

➢ Subpart A—General
  o 1803.1: Authority and purpose.
  o 1803.2: Definitions.
  o 1803.3: Contact for general information and requests.
  o 1803.4: Suggestions and complaints.
➢ Subpart B—Filing of Mandatory Declassification Review (MDR) Requests
  o 1803.11: Preliminary information.
  o 1803.12: Requirements as to form.
  o 1803.13: Fees.
➢ Subpart C—NACIC Action on MDR Requests
  o 1803.21: Receipt, recording, and tasking.
  o 1803.22: Requests barred by res judicata.
  o 1803.23: Determination by originator or interested party.
  o 1803.24: Notification of decision and right of appeal.
➢ Subpart D—NACIC Action on MDR Appeals
  o 1803.31: Requirements as to time and form.
  o 1803.32: Receipt, recording, and tasking.
  o 1803.33: Determination by NACIC Office Chiefs.
  o 1803.34: Appeal authority.
  o 1803.35: Action by appeals authority.
  o 1803.36: Notification of decision and right of further appeal.
➢ Subpart E—Further Appeals
  o 1803.41: Right of further appeal.

Authority:
Section 3.6 of Executive Order 12958 (or successor Orders) and Section 102 of the National Security Act, as amended (50 U.S.C. 403).

Source:
64 FR 49890, Sept. 14, 1999, unless otherwise noted.
SUBPART A—General
32 CFR Section 1803.1: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement § 3.6 of Executive Order (E.O.) 12958 (or successor Orders); and Section 102 of the National Security Act of 1947, as amended (50 U.S.C. 403).

(b) Purpose.

This part prescribes procedures, subject to limitations set forth below, for members of the public to request a declassification review of information classified under the various provisions of this or predecessor Orders. Section 3.6 of E.O. 12958 and these regulations do not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, officers, or employees.

32 CFR Section 1803.2: Definitions.
For purposes of this part, the following terms have the meanings as indicated:

NACIC

means the United States National Counterintelligence Center acting through the NACIC Information and Privacy Coordinator;

Days

means calendar days when NACIC is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any requirement of this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

Control

means ownership or the authority of NACIC pursuant to federal statute or privilege to regulate official or public access to records;

Coordinator

means the NACIC Information and Privacy Coordinator who serves as the NACIC manager of the information review and release program instituted under the mandatory declassification review provisions of Executive Order 12958;
Federal agency

means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

Information

means any knowledge that can be communicated or documentary material, regardless of its physical form that is owned by, produced by or for, or under the control of the United States Government; it does not include information originated by the incumbent President, White House Staff, appointed committees, commissions or boards, or any entities within the Executive Office that solely advise and assist the incumbent President;

Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of NACIC, has a subject matter or physical interest in the documents or information at issue;

NARA

means the National Archives and Records Administration;

Originator

means the NACIC officer who originated the information at issue, or successor in office, or a NACIC officer who has been delegated declassification authority for the information at issue in accordance with the provisions of this Order;

Presidential libraries

means the libraries or collection authorities established by statute to house the papers of former Presidents Hoover, Roosevelt, Truman, Eisenhower, Kennedy, Johnson, Nixon, Ford, Carter, Reagan, Bush and similar institutions or authorities as may be established in the future;

Referral

means coordination with or transfer of action to an interested party;
This Order

means Executive Order 12958 of April 17, 1995 or successor Orders;

32 CFR Section 1803.3: Contact for general information and requests.
For general information on this part or to request a declassification review, please direct your communication to the Information and Privacy Coordinator, National Counterintelligence Center, 3W01 NHB, Washington, DC 20505. Such inquiries will also be accepted by facsimile at (703) 874-5844. For general or status information only, the telephone number is (703) 874-4121. Collect calls cannot be accepted.

32 CFR Section 1803.4: Suggestions and complaints.
NACIC welcomes suggestions or complaints with regard to its administration of the mandatory declassification review program established under Executive Order 12958. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. NACIC will respond to all substantive communications and take such actions as determined feasible and appropriate.
SUBPART B—Filing of Mandatory Declassification Review (MDR) Requests

32 CFR Section 1803.11: Preliminary information.
Members of the public shall address all communications to the point of contact specified above and clearly delineate the communication as a request under this part. Requests and appeals on requests received from members of the public who owe outstanding fees for information services under this Order or the Freedom of Information Act at this or another federal agency will not be accepted until such debts are resolved.

32 CFR Section 1803.12: Requirements as to form.
The request shall identify the document(s) or material(s) with sufficient specificity (e.g., National Archives and Records Administration (NARA) Document Accession Number or other applicable, unique document identifying number) to enable NACIC to locate it with reasonable effort. Broad or topical requests for records on a particular subject may not be accepted under this provision. A request for documents contained in the various Presidential libraries shall be effected through the staff of such institutions who shall forward the document(s) in question for NACIC review. The requester shall also provide sufficient personal identifying information when required by NACIC to satisfy requirements of this part.

32 CFR Section 1803.13: Fees.
Requests submitted via NARA or the various Presidential libraries shall be responsible for reproduction costs required by statute or regulation. Requests made directly to NACIC will be liable for costs in the same amount and under the same conditions as specified in part 1800 of this chapter.
SUBPART C—NACIC Action on MDR Requests

32 CFR Section 1803.21: Receipt, recording, and tasking.
The Information and Privacy Coordinator shall within ten (10) days record each mandatory declassification review request received under this part, acknowledge receipt to the requester in writing (if received directly from a requester), and shall thereafter task the originator and other interested parties. Additional taskings, as required during the review process, shall be accomplished within ten (10) days of notification.

32 CFR Section 1803.22: Requests barred by res judicata.
The Coordinator shall respond to the requester and deny any request where the information in question has been the subject of a classification review within the previous two (2) years or is the subject of pending litigation in the federal courts.

32 CFR Section 1803.23: Determination by originator or interested party.

(a) In general.

The originator of the classified information (document) is a required party to any mandatory declassification review request; other interested parties may become involved through a referral by the Coordinator when it is determined that some or all of the information is also within their official cognizance.

(b) Required determinations.

These parties shall respond in writing to the Coordinator with a finding as to the classified status of the information including the category of protected information as set forth in § 1.5 of this Order, and, if older than ten (10) years, the basis for the extension of classification time under §§ 1.6 and 3.4 of this Order. These parties shall also provide a statement as to whether or not there is any other statutory, common law, or Constitutional basis for withholding as required by § 6.1(c) of this Order.

(c) Time.

This response shall be provided expeditiously on a first-in, first-out basis taking into account the business requirements of the originator or interested parties and consistent with the information rights of members of the general public under the Freedom of Information Act and the Privacy Act.

32 CFR Section 1803.24: Notification of decision and right of appeal.
The Coordinator shall communicate the decision of NACIC to the requester within ten (10) days of completion of all review action. That correspondence shall include a notice of a right of administrative appeal to the Director, NACIC pursuant to § 3.6(d) of this Order.
SUBPART D—NACIC Action on MDR Appeals

32 CFR Section 1803.31: Requirements as to time and form.
Appeals of decisions must be received by the Coordinator within forty-five (45) days of the date of mailing of NACIC's initial decision. It shall identify with specificity the documents or information to be considered on appeal and it may, but need not, provide a factual or legal basis for the appeal.

32 CFR Section 1803.32: Receipt, recording, and tasking.
The Coordinator shall promptly record each appeal received under this part, acknowledge receipt to the requester, and task the originator and other interested parties. Additional taskings, as required during the review process, shall be accomplished within ten (10) days of notification.

32 CFR Section 1803.33: Determination by NACIC Office Chiefs.
Each NACIC Office Chief in charge of an office which originated or has an interest in any of the records subject to the appeal, or designee, is a required party to any appeal; other interested parties may become involved through the request of the Coordinator when it is determined that some or all of the information is also within their official cognizance. These parties shall respond in writing to the Coordinator with a finding as to the classified status of the information including the category of protected information as set forth in § 1.5 of this Order, and, if older than ten (10) years, the basis for continued classification under §§ 1.6 and 3.4 of this Order. These parties shall also provide a statement as to whether or not there is any other statutory, common law, or Constitutional basis for withholding as required by § 6.1(c) of this Order. This response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the parties and consistent with the information rights of members of the general public under the Freedom of Information Act and the Privacy Act.

32 CFR Section 1803.34: Appeal authority.
The Director, NACIC will make final NACIC decisions from appeals of initial denial decisions under E.O. 12958. Matters decided by the Director, NACIC will be deemed a final decision by NACIC.

32 CFR Section 1803.35: Action by appeals authority.
Action by the Director, NACIC. The Coordinator shall provide a summation memorandum for consideration of the Director, NACIC; the complete record of the request consisting of the request, the document(s) (sanitized and full text) at issue, and the findings of the originator and interested parties. The Director, NACIC shall personally decide each case; no personal appearances shall be permitted without the express permission of the Director, NACIC.

32 CFR Section 1803.36: Notification of decision and right of further appeal.
The Coordinator shall communicate the decision of the Director, NACIC to the requester, NARA, or the particular Presidential Library within ten (10) days of such decision. That correspondence shall include a notice that an appeal of the decision may be made to the Interagency Security Classification Appeals Panel (ISCAP) established pursuant to § 5.4 of this Order.
SUBPART E—Further Appeals
32 CFR Section 1803.41: Right of further appeal.
A right of further appeal is available to the ISCAP established pursuant to § 5.4 of this Order. Action by that Panel will be the subject of rules to be promulgated by the Information Security Oversight Office (ISOO).
Subpart A—General
- 1804.01: Authority and purpose.
- 1804.02: Definitions.
- 1804.03: Contact for general information and requests.
- 1804.04: Suggestions and complaints.

Subpart B—Requests for Historical Access
- 1804.11: Requirements as to who may apply.
- 1804.12: Designations of authority to hear requests.
- 1804.13: Receipt, recording, and tasking.
- 1804.14: Determinations by tasked officials.
- 1804.15: Action by hearing authority.
- 1804.16: Action by appeal authority.
- 1804.17: Notification of decision.
- 1804.18: Termination of access.

Authority:

Source:
64 FR 49892, Sept. 14, 1999, unless otherwise noted.
SUBPART A—General
32 CFR Section 1804.1: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement § 4.5 of Executive Order 12958 (or successor Orders); and Presidential Decision Directive/NSC 24, U.S. Counterintelligence Effectiveness, dated May 3, 1994.

(b) Purpose.

(1) This part prescribes procedures for:
(i) Requesting access to NACIC records for purposes of historical research, or
(ii) Requesting access to NACIC records as a former Presidential appointee.
(2) Section 4.5 of Executive Order 12958 and this part do not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, officers, or employees.

32 CFR Section 1804.2: Definitions.
For purposes of this part, the following terms have the meanings indicated:

NACIC

means the United States National Counterintelligence Center acting through the NACIC Information and Privacy Coordinator;

Days

means calendar days when NACIC is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any requirement of this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

Control

means ownership or the authority of NACIC pursuant to federal statute or privilege to regulate official or public access to records;

Coordinator

means the NACIC Information and Privacy Coordinator who serves as the NACIC manager of the historical access program established pursuant to Section 4.5 of this Order;
Federal agency

means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

Former Presidential appointee

means any person who has previously occupied a policy-making position in the executive branch of the United States Government to which they were appointed by the current or former President and confirmed by the United States Senate;

Historian or historical researcher

means any individual with professional training in the academic field of history (or related fields such as journalism) engaged in a research project leading to publication (or any similar activity such as academic course development) reasonably intended to increase the understanding of the American public into the operations and activities of the United States government;

Information

means any knowledge that can be communicated or documentary material, regardless of its physical form that is owned by, produced by or for, or is under the control of the United States Government;

Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of NACIC, has a subject matter or physical interest in the documents or information at issue;

Originator

means the NACIC officer who originated the information at issue, or successor in office, or a NACIC officer who has been delegated declassification authority for the information at issue in accordance with the provisions of this Order;

This Order

means Executive Order 12958 of April 17, 1995 or successor Orders.
32 CFR Section 1804.3: Contact for general information and requests.
For general information on this part, to inquire about historical access to NACIC records, or to make a formal request for such access, please direct your communication in writing to the Information and Privacy Coordinator, Executive Secretariat, 3W01 NHB, National Counterintelligence Center, Washington, DC 20505. Inquiries will also be accepted by facsimile at (703) 874-5844. For general information only, the telephone number is (703) 874-4121. Collect calls cannot be accepted.

32 CFR Section 1804.4: Suggestions and complaints.
NACIC welcomes suggestions or complaints with regard to its administration of the historical access program established pursuant to Executive Order 12958. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. NACIC will respond to all substantive communications and take such actions as determined feasible and appropriate.
SUBPART B—Requests for Historical Access
32 CFR Section 1804.11: Requirements as to who may apply.

(a) Historical researchers:

(1) In general.
Any historian engaged in a historical research project as defined above may submit a request in writing to the Coordinator to be given access to classified information for purposes of that research. Any such request shall indicate the nature, purpose, and scope of the research project.

(2) Additional considerations.
In light of the very limited resources for NACIC's various historical programs, it is the policy of NACIC to consider applications for historical research privileges only in those instances where the researcher's needs cannot be satisfied through requests for access to reasonably described records under the Freedom of Information Act or the mandatory declassification review provisions of Executive Order 12958 and where issues of internal resource availability and fairness to all members of the historical research community militate in favor of a particular grant.

(b) Former Presidential appointees.

Any former Presidential appointee as defined herein may also submit a request to be given access to any classified records which they originated, reviewed, signed, or received while serving in that capacity. Such appointees may also request approval for a research associate but there is no entitlement to such enlargement of access and the decision in this regard shall be in the sole discretion of NACIC. Requests from appointees shall be in writing to the Coordinator and shall identify the records of interest.

32 CFR Section 1804.12: Designations of authority to hear requests.
The Director, NACIC has designated the Coordinator, as the NACIC authority to decide requests for historical and former Presidential appointee access under Executive Order 12958 (or successor Orders) and this part.

32 CFR Section 1804.13: Receipt, recording, and tasking.
The Information and Privacy Coordinator shall within ten (10) days record each request for historical access received under this part, acknowledge receipt to the requester in writing and take the following action:

(a) Compliance with general requirements.

The Coordinator shall review each request under this part and determine whether it meets the general requirements as set forth in § 1804.11; if it does not,
the Coordinator shall so notify the requester and explain the legal basis for this decision.

(b) Action on requests meeting general requirements.

For requests which meet the requirements of § 1804.11, the Coordinator shall thereafter task the originator(s) of the materials for which access is sought and other interested parties. Additional taskings, as required during the review process, shall be accomplished within ten (10) days of notification.

32 CFR Section 1804.14: Determinations by tasked officials.

(a) Required determinations.

The tasked parties as specified below shall respond in writing to the Coordinator with recommended findings to the following issues:
(1) That a serious professional or scholarly research project by the requester is contemplated;
(2) That such access is clearly consistent with the interests of national security (by originator and interested party, if any);
(3) That a non-disclosure agreement has been or will be executed by the requester (or research associate, if any) and other appropriate steps have been taken to assure that classified information will not be disclosed or otherwise compromised;
(4) That a pre-publication agreement has been or will be executed by the requester (or research associate, if any) which provides for a review of notes and any resulting manuscript by the Deputy Director of NACIC;
(5) That the information requested is reasonably accessible and can be located and compiled with a reasonable effort (by the Deputy Director of NACIC and the originator);
(6) That it is reasonably expected that substantial and substantive government documents and/or information will be amenable to declassification and release and/or publication (by the Deputy Director of NACIC and the originator);
(7) That sufficient resources are available for the administrative support of the researcher given current mission requirements (by the Deputy Director of NACIC and the originator); and,
(8) That the request cannot be satisfied to the same extent through requests for access to reasonably described records under the Freedom of Information Act or the mandatory declassification review provisions of Executive Order 12958 (by the Coordinator, the Deputy Director of NACIC and the originator).

(b) Time.

These responses shall be provided expeditiously on a first-in, first-out basis taking into account the business requirements of the tasked offices and consistent with the information rights of members of the general public under the Freedom of Information Act and the Privacy Act. NACIC will utilize its best efforts to
complete action on requests under this part within thirty (30) days of date of receipt.

32 CFR Section 1804.15: Action by hearing authority. Action by Coordinator. The Coordinator shall provide a summation memorandum for consideration of the Director, NACIC, the complete record of the request consisting of the request and the findings of the tasked parties. The Director, NACIC shall decide requests on the basis of the eight factors enumerated at § 1804.14(a). The Director, NACIC shall personally decide each case; no personal appearances shall be permitted without the express permission of the Director, NACIC.

32 CFR Section 1804.16: Action by appeal authority. The record compiled (the request, the memoranda filed by the originator and interested parties, and the previous decision(s)) as well as any memorandum of law or policy the referent desires to be considered, shall be certified by the Coordinator and shall constitute the official record of the proceedings and must be included in any subsequent filings. In such cases, the factors to be determined as specified in § 1804.14(a) will be considered by the Director, NACIC de novo and that decision shall be final.

32 CFR Section 1804.17: Notification of decision. The Coordinator shall inform the requester of the decision of the Director, NACIC within ten (10) days of the decision and, if favorable, shall manage the access for such period as deemed required but in no event for more than two (2) years unless renewed by the Director, NACIC in accordance with the requirements of § 1804.14(a).

32 CFR Section 1804.18: Termination of access. The Coordinator shall cancel any authorization whenever the security clearance of a requester (or research associate, if any) has been canceled or whenever the Director, NACIC determines that continued access would not be in compliance with one or more of the requirements of § 1804.14(a).
32 CFR PART 1805—PRODUCTION OF OFFICIAL RECORDS OR DISCLOSURE OF OFFICIAL INFORMATION IN PROCEEDINGS BEFORE FEDERAL, STATE OR LOCAL GOVERNMENT ENTITIES OF COMPETENT JURISDICTION

- 1805.1: Scope and purpose.
- 1805.2: Definitions.
- 1805.3: General.
- 1805.4: Procedures for production.

**Authority:**

**Source:**
64 FR 49894, Sept. 14, 1999, unless otherwise noted.
32 CFR Section 1805.1: Scope and purpose.
This part sets forth the policy and procedures with respect to the production or disclosure of:
(a) Material contained in the files of NACIC,
(b) Information relating to or based upon material contained in the files of NACIC,
(c) Information acquired by any person while such person is an employee of NACIC as part of the performance of that person’s official duties or because of that person’s association with NACIC.

32 CFR Section 1805.2: Definitions.
For the purpose of this part:

NACIC

means the National Counterintelligence Center and includes all staff elements of the NACIC.

Demand

means any subpoena, order or other legal summons (except garnishment orders) that is issued by a federal, state or local government entity of competent jurisdiction with the authority to require a response on a particular matter, or a request for appearance of an individual where a demand could issue.

Employee

means any officer, any staff, contract or other employee of NACIC, any person including independent contractors associated with or acting on behalf of NACIC; and any person formerly having such relationships with NACIC.

Production or produce

means the disclosure of:
(1) Any material contained in the files of NACIC; or
(2) Any information relating to material contained in the files of NACIC, including but not limited to summaries of such information or material, or opinions based on such information or material; or
(3) Any information acquired by persons while such persons were employees of NACIC as a part of the performance of their official duties or because of their official status or association with NACIC; in response to a demand upon an employee of NACIC.
is the NACIC employee designated to manage legal matters and regulatory compliance.

32 CFR Section 1805.3: General.
(a) No employee shall produce any materials or information in response to a demand without prior authorization as set forth in this part. This part also applies to former employees to the extent consistent with applicable non-disclosure agreements.
(b) This part is intended only to provide procedures for responding to demands for production of documents or information, and is not intended to, does not, and may not be relied upon to, create any right or benefit, substantive or procedural, enforceable by any party against the United States.

32 CFR Section 1805.4: Procedure for production.
(a) Whenever a demand for production is made upon an employee, the employee shall immediately notify NACIC Counsel, who will follow the procedures set forth in this section.
(b) NACIC Counsel and the Office Chiefs with responsibility for the information sought in the demand shall determine whether any information or materials may properly be produced in response to the demand, except that NACIC Counsel may assert any and all legal defenses and objections to the demand available to NACIC prior to the start of any search for information responsive to the demand. NACIC may, in its sole discretion, decline to begin any search for information responsive to the demand until a final and non-appealable disposition of any such defenses and objections raised by NACIC has been made by the entity or person that issued the demand.
(c) NACIC officials shall consider the following factors, among others, in reaching a decision:
(1) Whether production is appropriate in light of any relevant privilege;
(2) Whether production is appropriate under the applicable rules of discovery or the procedures governing the case or matter in which the demand arose; and
(3) Whether any of the following circumstances apply:
(i) Disclosure would violate a statute, including but not limited to the Privacy Act of 1974, as amended, 5 U.S.C. 552a;
(ii) Disclosure would reveal classified information;
(iii) Disclosure would improperly reveal trade secrets or proprietary confidential information without the owner’s consent; or
(iv) Disclosure would interfere with the orderly conduct of NACIC's functions.
(d) If oral or written testimony is sought by a demand in a case or matter in which the NACIC is not a party, a reasonably detailed description of the testimony sought, in the form of an affidavit or, if that is not feasible, a written statement, by the party seeking the testimony or by the party’s attorney must be furnished to the NACIC Counsel.
(e) The NACIC Counsel shall be responsible for notifying the appropriate employees and other persons of all decisions regarding responses to demands and providing advice and counsel as to the implementation of such decisions.

(f) If response to a demand is required before a decision is made whether to provide the documents or information sought by the demand, NACIC Counsel, after consultation with the Department of Justice, shall appear before and furnish the court or other competent authority with a copy of this part and state that the demand has been or is being, as the case may be, referred for the prompt consideration of the appropriate NACIC officials, and shall respectfully request the court or other authority to stay the demand pending receipt of the required instructions.

(g) If the court or any other authority declines to stay the demand pending receipt of instructions in response to a request made in accordance with § 1805.4(g) or rules that the demand must be complied with regardless of instructions rendered in accordance with this part not to produce the material or disclose the information sought, the employee upon whom the demand has been made shall, if so directed by NACIC Counsel, respectfully decline to comply with the demand under the authority of United States ex. rel. Touhy v. Ragen, 340 U.S. 462 (1951), and this part.

(h) With respect to any function granted to NACIC officials in this part, such officials are authorized to delegate in writing their authority in any case or matter or category thereof to subordinate officials.

(i) Any non-employee who receives a demand for the production or disclosure of NACIC information acquired because of that person’s association or contacts with NACIC should notify NACIC Counsel, (703) 874-4121, for guidance and assistance. In such cases, the provisions of this part shall be applicable.
32 CFR PART 1806—PROCEDURES GOVERNING ACCEPTANCE OF SERVICE OF PROCESS

➤ 1806.1: Scope and Purpose.
➤ 1806.2: Definitions.
➤ 1806.3: Procedures governing acceptance of service of process.
➤ 1806.4: Notification to NACIC Counsel.
➤ 1806.5: Authority of NACIC Counsel.

Authority:

Source:
64 FR 49895, Sept. 14, 1999, unless otherwise noted.

32 CFR Section 1806.1: Scope and purpose.
(a) This part sets forth the authority of NACIC personnel to accept service of process on behalf of the NACIC or any NACIC employee.
(b) This part is intended to ensure the orderly execution of the NACIC's affairs and not to impede any legal proceeding.
(c) NACIC regulations concerning employee responses to demands for production of official information before federal, state or local government entities are set out in part 1805 of this chapter.

32 CFR Section 1806.2: Definitions.

NACIC
means the National Counterintelligence Center and include all staff elements of NACIC.

Process
means a summons complaint, subpoena, or other official paper (except garnishment orders) issued in conjunction with a proceeding or hearing being conducted by a federal, state, or local government entity of competent jurisdiction.

Employee
means any NACIC officer, any staff, contract, or other employee of NACIC, any person including independent contractors associated with or acting for or on behalf of NACIC, and any person formerly having such a relationship with NACIC.

NACIC Counsel

refers to the NACIC employee designated by NACIC to manage legal issues and regulatory compliance.

32 CFR Section 1806.3: Procedures governing acceptance of service of process.

(a) Service of Process Upon the NACIC or a NACIC Employee in an Official Capacity

(1) Personal Service.
Unless otherwise expressly authorized by NACIC Counsel, or designee, personal service of process may be accepted only by NACIC Counsel, Director, NACIC, or Deputy Director, NACIC, located at Central Intelligence Agency Headquarters, Langley, Virginia.

(2) Mail Service.
Where service of process by registered or certified mail is authorized by law, unless expressly directed otherwise by the NACIC Counsel or designee, personal service of process may be accepted only by NACIC Counsel, Director, NACIC, or Deputy Director, NACIC. Process by mail should be addressed as follows: NACIC Counsel, National Counterintelligence Center, Washington, DC 20505.

(b) Service of Process Upon a NACIC Employee Solely in An Individual Capacity

(1) General.
NACIC will not provide the name or address of any current or former NACIC employee to individuals or entities seeking to serve process upon such employee solely in his or her individual capacity, even when the matter is related to NACIC activities.

(2) Personal Service.
Subject to the sole discretion of appropriate officials of the CIA, where NACIC is physically located, process servers generally will not be allowed to enter CIA Headquarters for the purpose of serving process upon any NACIC employee solely in his or her individual capacity. Subject to the sole discretion of the Director, NACIC, process servers will generally not be permitted to enter NACIC office space for the purpose of serving process upon a NACIC employee solely in his or her individual capacity. The NACIC Counsel, the Director, NACIC, and the Deputy Director, NACIC are not permitted to accept service of process on behalf of a NACIC employee in his or her individual capacity.
(3) Mail Service.
Unless otherwise expressly authorized by the NACIC Counsel, or designee, NACIC personnel are not authorized to accept or forward mailed service of process directed to any NACIC employee in his or her individual capacity. Any such process will be returned to the sender via appropriate postal channels.

(c) Service of Process Upon a NACIC Employee in a Combined Official and Individual Capacity

—Unless expressly directed otherwise by the NACIC Counsel, or designee, any process to be served upon a NACIC employee in his or her combined official and individual capacity, in person or by mail, can be accepted only by NACIC Counsel, Director, NACIC, or Deputy Director, NACIC, National Counterintelligence Center, Langley, Virginia.

(d) Service of Process Upon a NACIC Counsel.

The documents for which service is accepted in official capacity only shall be stamped “Service Accepted in Official Capacity Only.” Acceptance of Service of Process shall not constitute an admission or waiver with respect to jurisdiction, propriety of service, improper venue, or any other defense in law or equity available under the laws or rules applicable to the service of process.

32 CFR Section 1806.4: Notification to NACIC Counsel.
A NACIC employee who receives or has reason to expect to receive service of process in an individual, official, or combined individual and official capacity, in a matter that may involve or the furnishing of documents and that could reasonably be expected to involve NACIC interests, shall promptly notify the NACIC Counsel. Such notification should be given prior to providing the requestor, personal counsel or any other representative, any NACIC information and prior to the acceptance of service of process.

32 CFR Section 1806.5: Authority of NACIC Counsel.
Any questions concerning interpretation of this part shall be referred to the NACIC Counsel for resolution.
32 CFR PART 1807—ENFORCEMENT OF NONDISCRIMINATION ON THE BASIS OF DISABILITY IN PROGRAMS OR ACTIVITIES CONDUCTED BY THE NATIONAL COUNTERINTELLIGENCE CENTER

- 1807.101: Purpose.
- 1807.102: Application.
- 1807.103: Definitions.
- 1807.104-1807.110: [Reserved]
- 1807.111: Notice.
- 1807.112-1807.129: [Reserved]
- 1807.130: General prohibitions against discrimination.
- 1807.131-1807.139: [Reserved]
- 1807.140: Employment.
- 1807.141-1807.148: [Reserved]
- 1807.149: Program accessibility: discrimination prohibited.
- 1807.150: Program accessibility: existing facilities.
- 1807.151: Program accessibility: new construction and alterations.
- 1807.152-1807.159: [Reserved]
- 1807.160: Communications.
- 1807.161-1807.169: [Reserved]
- 1807.170: Compliance procedures.

Authority:

Source:
64 FR 49896, Sept. 14, 1999, unless otherwise noted.

32 CFR Section 1807.101: Purpose.
The purpose of this part is to effectuate section 119 of the Rehabilitation, Comprehensive Services, and Developmental Disabilities Amendments of 1978, which amended section 504 of the Rehabilitation Act of 1973 to prohibit discrimination on the basis of disability in programs or activities conducted by Executive agencies or the United States Postal Service.

32 CFR Section 1807.102: Application.
This part applies to all programs or activities conducted by the NACIC.
32 CFR Section 1807.103: Definitions.
For purposes of this part, the following terms means—

**Assistant Attorney General**

means the Assistant Attorney General, Civil Rights Division, United States Department of Justice.

**Auxiliary aids**

means services or devices that enable persons with impaired sensory, manual, or speaking skills to have an equal opportunity to participate in, and enjoy the benefits of, programs or activities conducted by the NACIC. For example, auxiliary aids useful for persons with impaired vision include readers, materials in Braille, audio recordings, and other similar services and devices. Auxiliary aids useful for persons with impaired hearing include telephone handset amplifiers, telephones compatible with hearing aids, telecommunication devices for deaf persons (TDD's), interpreters, notetakers, written materials, and other similar services and devices. The CIA, where NACIC is physically located, may prohibit from any of its facilities any auxiliary aid, or category of auxiliary aid that the Center for CIA Security (CCS) determines creates a security risk or potential security risk. CCS reserves the right to examine any auxiliary aid brought into the NACIC facilities at CIA Headquarters.

**Complete complaint**

means a written statement that contains the complainant's name and address and describes the NACIC's alleged discriminatory action in sufficient detail to inform the NACIC of the nature and date of the alleged violation of section 504. It must be signed by the complainant or by someone authorized to do so on his or her behalf. Complaints filed on behalf of classes or third parties must describe or identify (by name, if possible) the alleged victims of discrimination.

**Director**

means the Director of NACIC or an official or employee of the NACIC acting for the Director under a delegation of authority.

**Facility**
means all or any portion of buildings, structures, equipment, roads, walks, parking lots, rolling stock or other conveyances or other real or personal property.

**Individual with disabilities**

means any person who has a physical or mental impairment that substantially limits one or more major life activities, has a record of such an impairment, or is regarded as having such an impairment. As used in this definition, the phrase—

(1) Physical or mental impairment includes—

(i) Any physiological disorder or condition, cosmetic disfigurement, or anatomical loss affecting one or more of the following body systems: Cardiovascular; Neurological; musculoskeletal; special sense organs; respiratory, including speech organs; reproductive; digestive; genitourinary; hemic and lymphatic; skin; and endocrine; or

(ii) Any mental or psychological disorder, such as mental retardation, organic brain syndrome, emotional or mental illness, and specific learning disabilities. The term physical or mental impairment includes, but is not limited to, such diseases and conditions as orthopedic, visual, speech, and hearing impairments, cerebral palsy, epilepsy, muscular dystrophy, multiple sclerosis, cancer, heart disease, diabetes, mental retardation, emotional illness, drug addiction, and alcoholism.

(2) Major life activities includes functions such as caring for one's self, performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, and working;

(3) Has a record of such an impairment means has a history of, or has been misclassified as having a mental or physical impairment that substantially limits one or more major life activities.

(4) Is regarded as having an impairment means—

(i) Has a physical or mental impairment that does not substantially limit major life activities but is treated by the NACIC as constituting such a limitation;

(ii) Has a physical or mental impairment that substantially limits major life activities only as a result of the attitudes of others toward the impairment; or

(iii) Has none of the impairments defined in paragraph (1) of this definition but is treated by the NACIC as having such an impairment.

**Qualified individual with disabilities**

means—

(1) With respect to any NACIC program or activity under which a person is required to perform services or to achieve a level of accomplishment, an individual with a handicap who meets the essential eligibility requirements and who can achieve the purpose of the program or activity without modifications in
the program or activity that the NACIC can demonstrate would result in a fundamental alteration in its nature;
(2) With respect to any other NACIC program or activity, an individual with disabilities who meets the essential eligibility requirements for participation in, or receipt of benefits from, that program or activity; and

(3) Qualified individual with a disability as that term is defined for purposes of employment in 29 CFR 1614.203(a)(6), which is made applicable to this part by § 1807.140.

Section 504


32 CFR Section 1807.104 - 1807.110: [Reserved]

32 CFR Section 1807.111: Notice.
The NACIC shall make available to employees, applicants, participants, beneficiaries, and other interested persons, such information regarding the provisions of this part and its applicability to the programs or activities conducted by the NACIC, and make that information available to them in such manner as the Director finds necessary to apprise those persons of the protections against discrimination assured them by section 504 and the regulations in this part.

32 CFR Section 1807.112 - 1807.129: [Reserved]

32 CFR Section 1807.130: General prohibitions against discrimination.
(a) No qualified individual with disabilities shall, on the basis of disability, be excluded from participation in, be denied the benefits of, or otherwise be subjected to discrimination under, any program or activity conducted by the NACIC.
(b)(1) The NACIC, in providing any aid, benefit, or service, may not, directly or through contractual, licensing, or other arrangements, on the basis of disability:
(i) Deny a qualified individual with disabilities the opportunity to participate in or benefit from the aid, benefit, or service;
(ii) Deny a qualified individual with disabilities an opportunity to obtain the same result, to gain the same benefit, to reach the same level of achievement as that provided to others;
(iii) Provide a qualified individual with disabilities with an aid, benefit, or service that is not as effective in affording equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement as that provided to others;
(iv) Provide different or separate aid, benefits, or services to individuals with disabilities or to any class of individuals with disabilities than is provided to others unless that action is necessary to provide qualified individuals with disabilities with aid, benefits, or services that are as effective as those provided to others;
(v) Deny a qualified individual with disabilities the opportunity to participate as a member of planning or advisory boards; or
(vi) Otherwise limit a qualified individual with disabilities in the enjoyment of any right, privilege, advantage, or opportunity enjoyed by others receiving the aid, benefit, or service.
(2) The NACIC may not deny a qualified individual with disabilities the opportunity to participate in programs or activities that are not separate or different, despite the existence of permissibly separate or different programs or activities.
(3) The NACIC may not, directly or through contractual or other arrangements, utilize criteria or methods of administration the purpose or effect of which would:
(i) Subject qualified individuals with disabilities to discrimination on the basis of disability; or
(ii) Defeat or substantially impair accomplishment of the objectives of a program or activity with respect to individuals with disabilities.
(4) The NACIC may not, in determining the site or location of a facility, make selections the purpose or effect of which would:
(i) Exclude individuals with disabilities from, deny them the benefits of, or otherwise subject them to discrimination under, any program or activity conducted by the NACIC; or
(ii) Defeat or substantially impair the accomplishment of the objectives of a program or activity with respect to individuals with disabilities.
(5) The NACIC, in the selection of procurement contractors, may not use criteria that subject qualified individuals with disabilities to discrimination on the basis of disability.
(6) The NACIC may not administer a licensing or certification program in a manner that subjects qualified individuals with disabilities to discrimination on the basis of disability, nor may the NACIC establish requirements for the programs or activities of licensees or certified entities that subject qualified individuals with disabilities to discrimination on the basis of disability. However, the programs or activities of entities that are licensed or certified by the NACIC are not, themselves, covered by this part.
(c) The exclusion of persons without disabilities from the benefits of a program limited by Federal statute or Executive Order to individuals with disabilities or
the exclusion of a specific class of individuals with disabilities from a program limited by Federal statute or Executive Order to a different class of individuals with disabilities is not prohibited by this part.  
(d) The NACIC shall administer programs and activities in the most integrated setting appropriate to the needs of qualified individuals with disabilities.

32 CFR Section 1807.131 - 1807.139: [Reserved]

32 CFR Section 1807.140: Employment.  
No qualified individual with disabilities shall, solely on the basis of disability, be subjected to discrimination in employment under any program or activity conducted by the NACIC.  The definitions, requirements, and procedures of section 501 of the Rehabilitation Act of 1979 (29 U.S.C. 791), as established by the Equal Employment Opportunity Commission in 29 CFR part 1614, shall apply to employment in federally conducted programs or activities.

32 CFR Section 1807.141 - 1807.148: [Reserved]

32 CFR Section 1807.149: Program accessibility: discrimination prohibited.  
Except as otherwise provided in § 1807.150, no qualified individual with disabilities shall, because the NACIC's facilities are inaccessible to or unusable by individuals with disabilities, be denied the benefits of, be excluded from participation in, or otherwise be subjected to discrimination under any program or activity conducted by the NACIC.

32 CFR Section 1807.150: Program accessibility: existing facilities.  

(a) General.

The NACIC shall operate each program or activity so that the program or activity, viewed in its entirety, is readily accessible to and usable by individuals with disabilities.  This program does not:  
(1) Necessarily require the NACIC to make each of its existing facilities accessible to and usable by individuals with disabilities;  
(2)(i) Require the NACIC to take any action that it can demonstrate would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens.  
(ii) The NACIC has the burden of proving that compliance with § 1807.150(a) would result in that alteration or those burdens.  
(iii) The decision that compliance would result in that alteration of those burdens must be made by the Director after considering all of the NACIC's resources available for use in the funding and operation of the conducted program or activity, and must be accompanied by a written statement of the reasons for reaching that conclusion.
(iv) If an action would result in that alteration or those burdens, the NACIC shall take any other action that would not result in the alteration of burdens but would nevertheless ensure that individuals with disabilities receive the benefits and services of the program or activity.

(b) Methods.

(1) The NACIC may comply with the requirements of this section through such means as redesign of equipment, delivery of services at alternate accessible sites, alteration of existing facilities, or any other methods that result in making its programs or activities readily accessible to and usable by individuals with disabilities.

(2) The NACIC is not required to make structural changes in existing facilities if other methods are effective in achieving compliance with this section.

(3) In choosing among available methods for meeting the requirements of this section, the NACIC shall give priority to those methods that offer programs and activities to qualified individuals with disabilities in the most integrated setting appropriate.

32 CFR Section 1807.151: Program accessibility: new construction and alterations.
Each building or part of a building that is constructed or altered by, on behalf of, or for the use of, the NACIC shall be designed, constructed, or altered so as to be readily accessible to and usable by individuals with disabilities in compliance with the definitions, requirements, and standards of the Americans with Disabilities Act Accessibility Guidelines, 36 CFR part 1191.

32 CFR Section 1807.152 - 1807.159: [Reserved]

32 CFR Section 1807.160: Communications.
(a) The NACIC shall take appropriate steps to ensure effective communication with applicants, participants, personnel of other Federal entities, and members of the public as follows:
(1)(i) The NACIC shall furnish appropriate auxiliary aids if necessary to afford an individual with disabilities an equal opportunity to participate in, and enjoy the benefits of, a program or activity conducted by the NACIC.
(ii) In determining what type of auxiliary aid is necessary, the NACIC shall give primary consideration to the requests of the individual with disabilities.
(2) Where the NACIC communicates with applicants and beneficiaries by telephone, telecommunication devices for deaf persons (TDD’s) or equally effective telecommunication systems shall be used to communicate with persons with impaired hearing.
(b) The NACIC shall ensure that interested persons, including persons with impaired vision or hearing, can obtain information as to the existence and location of accessible services, activities, and facilities.
(c) This section does not require the NACIC to take any action that it can demonstrate would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens. In those circumstances where NACIC personnel believe that the proposed action would fundamentally alter the program or activity or would result in undue financial and administrative burdens, the NACIC has the burden of proving that compliance with § 1807.160 would result in such alteration or burdens. The decision that compliance would result in such alteration or burdens must be made by the NACIC head or his or her designee after considering all NACIC resources available for use in the funding and operation of the conducted program or activity and must be accompanied by a written statement of the reasons for reaching that conclusion. If an action required to comply with this section would result in such an alteration or such burdens, the NACIC shall take any other action that would not result in such an alteration or such burdens but would nevertheless ensure that, to the maximum extent possible, individuals with disabilities receive the benefits and services of the program or activity.

32 CFR Section 1807.161-1807.169: [Reserved]

32 CFR Section 1807.170: Compliance procedures.
(a) Except as provided in paragraph (b) of this section, this section applies to all allegations of discrimination on the basis of disability in programs and activities conducted by the NACIC.
(b) The NACIC shall process complaints alleging violations of section 504 with respect to employment according to the procedures established by the Equal Employment Opportunity Commission in 29 CFR part 1614 pursuant to section 501 of the Rehabilitation Act of 1973 (29 U.S.C. 791).
(c) The Director, Office of Equal Employment Opportunity, is responsible for coordinating implementation of this section. Complaints may be sent to NACIC, Director, Washington, DC 20505.
(d) The NACIC shall accept and investigate all complete complaints for which it has jurisdiction. All complete complaints must be filed within 180 days of the alleged act of discrimination. The NACIC may extend this time period for good cause.
(e) If the NACIC receives a complaint over which it does not have jurisdiction, it shall promptly notify the complainant and shall make reasonable efforts to refer the complaint to the appropriate government entity.
(f) The NACIC shall notify the Architectural and Transportation Barriers Compliance Board upon receipt of any complaint alleging that a building or facility that is subject to the Americans with Disabilities Act Accessibility Guidelines is not readily accessible to and usable by individuals with disabilities.
(g) Within 180 days of the receipt of a complete complaint for which it has jurisdiction, the NACIC shall notify the complainant of the results of the investigation in a letter containing:
(1) Findings of fact and conclusions of law;
(2) A description of a remedy for each violation found; and
(3) A notice of the right to appeal.

(h) Appeals of the findings of fact and conclusions of law or remedies must be filed by the complainant within 90 days of receipt from the NACIC of the letter required by paragraph (g) of this section. The NACIC may extend this time for good cause.

(i) Timely appeals shall be accepted and processed by the Director.

(j) The NACIC shall notify the complainant of the results of the appeal within 60 days of the receipt of the request. If the NACIC determines that it needs additional information from the complainant, it shall have 60 days from the date it receives the additional information to make its determination on the appeal.

(k) The time limits cited in paragraphs (g) and (j) of this section may be extended with the permission of the Assistant Attorney General.

(l) The Director may delegate the authority for conducting complaint investigations to other Federal agencies, except that the authority for making the final determination may not be delegated.
32 CFR CHAPTER XIX—CENTRAL INTELLIGENCE AGENCY

- 32 CFR Part 1900: Public access to CIA records under the Freedom of Information Act (FOIA)
- 32 CFR Part 1901: Public rights under the Privacy Act of 1974
- 32 CFR Part 1902: Information security regulations
- 32 CFR Part 1903: Conduct on Agency installations
- 32 CFR Part 1904: Procedures governing acceptance of service of process
- 32 CFR Part 1905: Production of official records or disclosure of official information in proceedings before Federal, State or local governmental entities of competent jurisdiction
- 32 CFR Part 1906: Enforcement of nondiscrimination on the basis of handicap in programs or activities conducted by the Central Intelligence Agency
- 32 CFR Part 1907: Challenges to classification of documents by authorized holders pursuant to § 1.9 of Executive Order 12958
- 32 CFR Part 1908: Public requests for mandatory declassification review of classified information pursuant to § 3.6 of Executive Order 12958
- 32 CFR Part 1909: Access by historical researchers and former presidential appointees pursuant to § 4.5 of Executive Order 12958
- 32 CFR Part 1910: Debarment and suspension procedures
32 CFR PART 1900—PUBLIC ACCESS TO CIA RECORDS UNDER THE FREEDOM OF INFORMATION ACT (FOIA)

- 32 CFR PART 1900—PUBLIC ACCESS TO CIA RECORDS UNDER THE FREEDOM OF INFORMATION ACT (FOIA)
  - 1900.01: Authority and purpose.
  - 1900.02: Definitions.
  - 1900.03: Contact for general information and requests.
  - 1900.04: Suggestions and complaints.

- Filing of FOIA Requests
  - 1900.11: Preliminary information.
  - 1900.12: Requirements as to form and content.
  - 1900.13: Fees for record services.
  - 1900.14: Fee estimates (pre-request option).

- CIA Action on FOIA Requests
  - 1900.21: Processing of requests for records.
  - 1900.22: Action and determination(s) by originator(s) or any interested party.
  - 1900.23: Payment of fees, notification of decision, and right of appeal.

- Additional Administrative Matters
  - 1900.31: Procedures for business information.
  - 1900.32: Procedures for information concerning other persons.
  - 1900.33: Allocation of resources; agreed extensions of time.
  - 1900.34: Requests for expedited processing.

- CIA Action on FOIA Administrative Appeals
  - 1900.41: Establishment of appeals structure.
  - 1900.42: Right of appeal and appeal procedures.
  - 1900.43: Determination(s) by Deputy Director(s).
  - 1900.44: Action by appeals authority.
  - 1900.45: Notification of decision and right of judicial review.

Authority:
National Security Act of 1947, as amended; Central Intelligence Agency Act of 1949, as amended; Freedom of Information Act, as amended; CIA Information Act of 1984; and Executive Order 12958, 60 FR 19825, 3 CFR 1996 Comp., p. 333-356 (or successor Orders).

Source:
62 FR 32481, June 16, 1997, unless otherwise noted.
32 CFR Section 1900.01: Authority and purpose.
This part is issued under the authority of and in order to implement the Freedom of Information Act (FOIA), as amended (5 U.S.C. 552); the CIA Information Act of 1984 (50 U.S.C. 431); sec. 102 of the National Security Act of 1947, as amended (50 U.S.C. 403); and sec. 6 of the Central Intelligence Agency Act of 1949, as amended (50 U.S.C. 403g). It prescribes procedures for:
(a) Requesting information on available CIA records, or the CIA administration of the FOIA, or estimates of fees that may become due as a result of a request;
(b) Requesting records pursuant to the FOIA; and
(c) Filing an administrative appeal of an initial adverse decision under the FOIA.

32 CFR Section 1900.02: Definitions.
For purposes of this part, the following terms have the meanings indicated:

(a) Agency or CIA

means the United States Central Intelligence Agency acting through the CIA Information and Privacy Coordinator;

(b) Days

means calendar days when the Agency is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

(c) Control

means ownership or the authority of the CIA pursuant to federal statute or privilege to regulate official or public access to records;

(d) Coordinator

means the CIA Information and Privacy Coordinator who serves as the Agency manager of the information review and release program instituted under the Freedom of Information Act;

(e) Direct costs

means those expenditures which an agency actually incurs in the processing of a FOIA request; it does not include overhead factors such as space; it does include:

(1) Pages
means paper copies of standard office size or the dollar value equivalent in other media;
(2) Reproduction
means generation of a copy of a requested record in a form appropriate for release;

(3) Review
means all time expended in examining a record to determine whether any portion must be withheld pursuant to law and in effecting any required deletions but excludes personnel hours expended in resolving general legal or policy issues; it also means personnel hours of professional time;

(4) Search
means all time expended in looking for and retrieving material that may be responsive to a request utilizing available paper and electronic indices and finding aids; it also means personnel hours of professional time or the dollar value equivalent in computer searches;

(f) Expression of interest
means a written communication submitted by a member of the public requesting information on or concerning the FOIA program and/or the availability of documents from the CIA;

(g) Federal agency
means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

(h) Fees
means those direct costs which may be assessed a requester considering the categories established by the FOIA; requesters should submit information to assist the Agency in determining the proper fee category and the Agency may draw reasonable inferences from the identity and activities of the requester in making such determinations; the fee categories include:

(1) Commercial
means a request in which the disclosure sought is primarily in the commercial interest of the requester and which furthers such commercial, trade, income or profit interests;

(2) Non-commercial educational or scientific institution
means a request from an accredited United States educational institution at any academic level or institution engaged in research concerning the social, biological, or physical sciences or an instructor or researcher or member of such institutions; it also means that the information will be used in a specific scholarly or analytical work, will contribute to the advancement of public knowledge, and will be disseminated to the general public;
(3) Representative of the news media

refers to any person actively gathering news for an entity that is organized and operated to publish or broadcast news to the public. The term “news” means information that is about current events or that would be of current interest to the public. Examples of news media entities include television or radio stations broadcasting to the public at large, and publishers of periodicals (but only in those instances when they can qualify as disseminators of “news”) who make their products available for purchase or subscription by the general public. These examples are not intended to be all-inclusive. Moreover, as traditional methods of news delivery evolve (e.g., electronic dissemination of newspapers through telecommunications services), such alternative media would be included in this category. In the case of “freelance” journalists, they may be regarded as working for a news organization if they can demonstrate a solid basis for expecting publication through that organization, even though not actually employed by it. A publication contract would be the clearest proof, but agencies may also look to the past publication record of a requestor in making this determination:

(4) All other

means a request from an individual not within paragraph (h)(1), (2), or (3) of this section;

(i) Freedom of Information Act

or “FOIA” means the statutes as codified at 5 U.S.C. 552;

(j) Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of the CIA, has a subject matter or physical interest in the documents or information at issue;

(k) Originator

means the U.S. Government official who originated the document at issue or successor in office or such official who has been delegated release or declassification authority pursuant to law;

(l) Potential requester

means a person, organization, or other entity who submits an expression of interest;

(m) Reasonably described records

means a description of a document (record) by unique identification number or descriptive terms which permit an Agency employee to locate documents with reasonable effort given existing indices and finding aids;
(n) Records or agency records

means all documents, irrespective of physical or electronic form, made or received by the CIA in pursuance of federal law or in connection with the transaction of public business and appropriate for preservation by the CIA as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the CIA or because of the informational value of the data contained therein; it does not include:

(1) Books, newspapers, magazines, journals, magnetic or printed transcripts of electronic broadcasts, or similar public sector materials acquired generally and/or maintained for library or reference purposes; to the extent that such materials are incorporated into any form of analysis or otherwise distributed or published by the Agency, they are fully subject to the disclosure provisions of the FOIA;

(2) Index, filing, or museum documents
made or acquired and preserved solely for reference, indexing, filing, or exhibition purposes; and

(3) Routing and transmittal sheets and notes and filing or destruction notes
which do not also include information, comment, or statements of substance;

(o) Responsive records

means those documents (i.e., records) which the Agency has determined to be within the scope of a FOIA request.


32 CFR Section 1900.03: Contact for general information and requests.  
For general information on this part, to inquire about the FOIA program at CIA, or to file a FOIA request (or expression of interest), please direct your communication in writing to the Information and Privacy Coordinator, Central Intelligence Agency, Washington, DC 20505. Such inquiries will also be accepted by facsimile at (703) 613-3007. For general information or status information on pending cases only, the telephone number is (703) 613-1287. Collect calls cannot be accepted.

32 CFR Section 1900.04: Suggestions and complaints.
The Agency welcomes suggestions or complaints with regard to its administration of the Freedom of Information Act. Many requesters will receive pre-paid, customer satisfaction survey cards. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. The Agency will
respond to all substantive communications and take such actions as determined feasible and appropriate.

Filing of FOIA Requests

32 CFR Section 1900.11: Preliminary Information. Members of the public shall address all communications to the CIA Coordinator as specified at 32 CFR 1900.03 and clearly delineate the communication as a request under the Freedom of Information Act and this regulation. CIA employees receiving a communication in the nature of a FOIA request shall expeditiously forward same to the Coordinator. Requests and appeals on requests, referrals, or coordinations received from members of the public who owe outstanding fees for information services at this or other federal agencies will not be accepted and action on all pending requests shall be terminated in such circumstances.

32 CFR Section 1900.12: Requirements as to form and content.

(a) Required information.

No particular form is required. A request need only reasonably describe the records of interest. This means that documents must be described sufficiently to enable a professional employee familiar with the subject to locate the documents with a reasonable effort. Commonly this equates to a requirement that the documents must be locatable through the indexing of our various systems. Extremely broad or vague requests or requests requiring research do not satisfy this requirement.

(b) Additional information for fee determination.

In addition, a requester should provide sufficient personal identifying information to allow us to determine the appropriate fee category. A requester should also provide an agreement to pay all applicable fees or fees not to exceed a certain amount or request a fee waiver.

(c) Otherwise.

Communications which do not meet these requirements will be considered an expression of interest and the Agency will work with, and offer suggestions to, the potential requester in order to define a request properly.

32 CFR Section 1900.13: Fees for record services.

(a) In general.

Search, review, and reproduction fees will be charged in accordance with the provisions below relating to schedule, limitations, and category of requester.
Applicable fees will be due even if our search locates no responsive records or some or all of the responsive records must be denied under one or more of the exemptions of the Freedom of Information Act.

(b) Fee waiver requests.

Records will be furnished without charge or at a reduced rate whenever the Agency determines:
(1) That, as a matter of administrative discretion, the interest of the United States Government would be served, or
(2) That it is in the public interest because it is likely to contribute significantly to the public understanding of the operations or activities of the United States Government and is not primarily in the commercial interest of the requester; the Agency shall consider the following factors when making this determination:
   (i) Whether the subject of the request concerns the operations or activities of the United States Government; and, if so,
   (ii) Whether the disclosure of the requested documents is likely to contribute to an understanding of United States Government operations or activities; and, if so,
   (iii) Whether the disclosure of the requested documents will contribute to public understanding of United States Government operations or activities; and,
   (iv) Whether the disclosure of the requested documents is likely to contribute significantly to public understanding of United States Government operations and activities; and
   (v) Whether the requester has a commercial interest that would be furthered by the requested disclosure; and, if so,
   (vi) Whether the disclosure is primarily in the commercial interest of the requester.

(c) Fee waiver appeals.

Denials of requests for fee waivers or reductions may be appealed to the Chair of the Agency Release Panel via the Coordinator. A requester is encouraged to provide any explanation or argument as to how his or her request satisfies the statutory requirement set forth above.

(d) Time for fee waiver requests and appeals.

It is suggested that such requests and appeals be made and resolved prior to the initiation of processing and the incurring of costs. However, fee waiver requests will be accepted at any time prior to the release of documents or the completion of a case, and fee waiver appeals within forty-five (45) days of our initial decision subject to the following condition: If processing has been initiated, then the requester must agree to be responsible for costs in the event of an adverse administrative or judicial decision.

(e) Agreement to pay fees.
In order to protect requesters from large and/or unanticipated charges, the Agency will request specific commitment when it estimates that fees will exceed $100.00. The Agency will hold in abeyance for forty-five (45) days requests requiring such agreement and will thereafter deem the request closed. This action, of course, would not prevent an individual from refiling his or her FOIA request with a fee commitment at a subsequent date.

(f) Deposits.

The Agency may require an advance deposit of up to 100 percent of the estimated fees when fees may exceed $250.00 and the requester has no history of payment, or when, for fees of any amount, there is evidence that the requester may not pay the fees which would be accrued by processing the request. The Agency will hold in abeyance for forty-five (45) days those requests where deposits have been requested.

(g) Schedule of fees

(1) In general.
The schedule of fees for services performed in responding to requests for records is established as follows:

Personnel Search and Review

Clerical/Technical
Quarter hour
$5.00

Professional/Supervisory
Quarter hour
10.00

Manager/Senior Professional
Quarter hour
18.00

Computer Search and Production
Search (on-line)
Flat rate
10.00

Search (off-line)
Flat rate
30.00
Other activity
Per minute
10.00

Tapes (mainframe cassette)
Each
9.00

Tapes (mainframe cartridge)
Each
9.00

Tapes (mainframe reel)
Each
20.00

Tapes (PC 9mm)
Each
25.00

Diskette (3.5”)
Each
4.00

CD (bulk recorded)
Each
10.00

CD (recordable)
Each
20.00

Telecommunications
Per minute
.50

Paper (mainframe printer)
Per page
.10

Paper (PC b&w laser printer)
Per page
.10

Paper (PC color printer)
Per page

Page 1014
Paper Production

Photocopy (standard or legal)
Per page
.10

Microfiche
Per frame
.20

Pre-printed (if available)
Per 100 pages
5.00

Published (if available)
Per item
NTIS

(2) Application of schedule.
Personnel search time includes time expended in either manual paper records searches, indices searches, review of computer search results for relevance, personal computer system searches, and various reproduction services. In any event where the actual cost to the Agency of a particular item is less than the above schedule (e.g., a large production run of a document resulted in a cost less than $5.00 per hundred pages), then the actual lesser cost will be charged. Items published and available at the National Technical Information Service (NTIS) are also available from CIA pursuant to this part at the NTIS price as authorized by statute.

(3) Other services.
For all other types of output, production, or reproduction (e.g., photographs, maps, or published reports), actual cost or amounts authorized by statute. Determinations of actual cost shall include the commercial cost of the media, the personnel time expended in making the item to be released, and an allocated cost of the equipment used in making the item, or, if the production is effected by a commercial service, then that charge shall be deemed the actual cost for purposes of this part.

(h) Limitations on collection of fees

(1) In general.
No fees will be charged if the cost of collecting the fee is equal to or greater than the fee itself. That cost includes the administrative costs to the Agency of billing,
receiving, recording, and processing the fee for deposit to the Treasury Department and, as of the date of these regulations, is deemed to be $10.00.

(2) Requests for personal information.
No fees will be charged for requesters seeking records about themselves under the FOIA; such requests are processed in accordance with both the FOIA and the Privacy Act in order to ensure the maximum disclosure without charge.

(i) Fee categories.

There are four categories of FOIA requesters for fee purposes: Commercial use requesters, educational and non-commercial scientific institution requesters, representatives of the news media requesters, and all other requesters. The categories are defined in § 1900.02, and applicable fees, which are the same in two of the categories, will be assessed as follows:

(1) Commercial use requesters:
Charges which recover the full direct costs of searching for, reviewing, and duplicating responsive records (if any);

(2) Educational and non-commercial scientific institution requesters as well as “representatives of the news media” requesters:
Only charges for reproduction beyond the first 100 pages;

(3) All other requesters:
Charges which recover the full direct cost of searching for and reproducing responsive records (if any) beyond the first 100 pages of reproduction and the first two hours of search time which will be furnished without charge.

(j) Associated requests.

A requester or associated requesters may not file a series of multiple requests, which are merely discrete subdivisions of the information actually sought for the purpose of avoiding or reducing applicable fees. In such instances, the Agency may aggregate the requests and charge the applicable fees.

32 CFR Section 1900.14: Fee estimates (pre-request option).
In order to avoid unanticipated or potentially large fees, a requester may submit a request for a fee estimate. The Agency will endeavor within ten (10) days to provide an accurate estimate, and, if a request is thereafter submitted, the Agency will not accrue or charge fees in excess of our estimate without the specific permission of the requester. Effective October 2, 1997, the ten (10) day provision is modified to twenty (20) days pursuant to the Electronic Freedom of Information Act Amendments of 1996.

CIA Action on FOIA Requests
32 CFR Section 1900.21: Processing of requests for records.

(a) In general.

Requests meeting the requirements of §§ 1900.11 through 1900.13 shall be accepted as formal requests and processed under the Freedom of Information Act, 5 U.S.C. 552, and these regulations. Upon receipt, the Agency shall within ten (10) days record each request, acknowledge receipt to the requester in writing, and thereafter effect the necessary taskings to the CIA components reasonably believed to hold responsive records. Effective October 2, 1997, the ten (10) day provision is modified to twenty (20) days pursuant to the Electronic Freedom of Information Act Amendments of 1996.

(b) Database of “officially released information.”

As an alternative to extensive tasking and as an accommodation to many requesters, the Agency maintains a database of “officially released information” which contains copies of documents released by this Agency. Searches of this database, containing currently in excess of 500,000 pages, can be accomplished expeditiously. Moreover, requests that are specific and well-focused will often incur minimal, if any, costs. Requesters interested in this means of access should so indicate in their correspondence. Effective November 1, 1997 and consistent with the mandate of the Electronic Freedom of Information Act Amendments of 1996, on-the-public. Detailed information regarding such access will line electronic access to these records will be available to be available at that time from the point of contact specified in § 1900.03.

(c) Effect of certain exemptions.

In processing a request, the Agency shall decline to confirm or deny the existence or nonexistence of any responsive records whenever the fact of their existence or nonexistence is itself classified under Executive Order 12958 or revealing of intelligence sources and methods protected pursuant to section 103(c)(5) of the National Security Act of 1947. In such circumstances, the Agency, in the form of a final written response, shall so inform the requester and advise of his or her right to an administrative appeal.

(d) Time for response.

The Agency will utilize every effort to determine within the statutory guideline of ten (10) days after receipt of an initial request whether to comply with such a request. However, the current volume of requests require that the Agency seek additional time from a requester pursuant to 32 CFR 1900.33. In such event, the Agency will inform the requester in writing and further advise of his or her right to file an administrative appeal of any adverse determination. Effective October 2, 1997, the ten (10) day provision is modified to twenty (20) days pursuant to the Electronic Freedom of Information Act Amendments of 1996.
32 CFR Section 1900.22: Action and determination(s) by originator(s) or any interested party.

(a) Initial action for access.

CIA components tasked pursuant to a FOIA request shall search all relevant record systems within their cognizance which have not been excepted from search by the provisions of the CIA Information Act of 1984. They shall:
(1) Determine whether a record exists;
(2) Determine whether and to what extent any FOIA exemptions apply;
(3) Approve the disclosure of all non-exempt records or portions of records for which they are the originator; and
(4) Forward to the Coordinator all records approved for release or necessary for coordination with or referral to another originator or interested party. In making these decisions, the CIA component officers shall be guided by the applicable law as well as the procedures specified at 32 CFR 1900.31 and 32 CFR 1900.32 regarding confidential commercial information and personal information (about persons other than the requester).

(b) Referrals and coordinations.

As applicable and within ten (10) days of receipt by the Coordinator, any CIA records containing information originated by other CIA components shall be forwarded to those entities for action in accordance with paragraph (a) of this section and return. Records originated by other federal agencies or CIA records containing other federal agency information shall be forwarded to such agencies within ten (10) days of our completion of initial action in the case for action under their regulations and direct response to the requester (for other agency records) or return to the CIA (for CIA records). Effective October 2, 1997, the ten (10) day provision is modified to twenty (20) days pursuant to the Electronic Freedom of Information Act Amendments of 1996.

32 CFR Section 1900.23: Payment of fees, notification of decision, and right of appeal.

(a) Fees in general.

Fees collected under this part do not accrue to the Central Intelligence Agency and shall be deposited immediately to the general account of the United States Treasury.

(b) Notification of decision.

Upon completion of all required review and the receipt of accrued fees (or promise to pay such fees), the Agency will promptly inform the requester in writing of those records or portions of records which may be released and which
must be denied. With respect to the former, the Agency will provide copies; with respect to the latter, the Agency shall explain the reasons for the denial, identify the person(s) responsible for such decisions by name and title, and give notice of a right of administrative appeal.

(c) Availability of reading room.

As an alternative to receiving records by mail, a requester may arrange to inspect the records deemed releasable at a CIA “reading room” in the metropolitan Washington, DC area. Access will be granted after applicable and accrued fees have been paid. Requests to review or browse documents in our database of “officially released records” will also be honored in this manner to the extent that paper copies or electronic copies in unclassified computer systems exist. All such requests shall be in writing and addressed pursuant to 32 CFR 1900.03. The records will be available at such times as mutually agreed but not less than three (3) days from our receipt of a request. The requester will be responsible for reproduction charges for any copies of records desired.

Additional Administrative Matters

32 CFR Section 1900.31: Procedures for business information.

(a) In general.

Business information obtained by the Central Intelligence Agency by a submitter shall not be disclosed pursuant to a Freedom of Information Act request except in accordance with this section. For purposes of this section, the following definitions apply:

(1) Business information
means commercial or financial information in which a legal entity has a recognized property interest;

(2) Confidential commercial information
means such business information provided to the United States Government by a submitter which is reasonably believed to contain information exempt from release under exemption (b)(4) of the Freedom of Information Act, 5 U.S.C. 552, because disclosure could reasonably be expected to cause substantial competitive harm;

(3)Submitter
means any person or entity who provides confidential commercial information to the United States Government; it includes, but is not limited to, corporations, businesses (however organized), state governments, and foreign governments; and

(b) Designation of confidential commercial information.
A submitter of business information will use good-faith efforts to designate, by appropriate markings, either at the time of submission or at a reasonable time thereafter, any portions of its submission that it considers to be confidential commercial information and hence protected from required disclosure pursuant to exemption (b)(4). Such designations shall expire ten (10) years after the date of the submission unless the submitter requests, and provides justification for, a longer designation period.

(c) Process in event of FOIA request

(1) Notice to submitters.
The Agency shall provide a submitter with prompt written notice of receipt of a Freedom of Information Act request encompassing business information whenever:
(i) The submitter has in good faith designated the information as confidential commercial information, or

(ii) The Agency believes that disclosure of the information could reasonably be expected to cause substantial competitive harm, and
(iii) The information was submitted within the last ten (10) years unless the submitter requested and provided acceptable justification for a specific notice period of greater duration.

(2) Form of notice.
This notice shall either describe the exact nature of the confidential commercial information at issue or provide copies of the responsive records containing such information.

(3) Response by submitter.
(i) Within seven (7) days of the above notice, all claims of confidentiality by a submitter must be supported by a detailed statement of any objection to disclosure. Such statement shall:
(A) Specify that the information has not been disclosed to the public;
(B) Explain why the information is contended to be a trade secret or confidential commercial information;
(C) Explain how the information is capable of competitive damage if disclosed;
(D) State that the submitter will provide the Agency and the Department of Justice with such litigation defense as requested; and
(E) Be certified by an officer authorized to legally bind the corporation or similar entity.
(ii) It should be noted that information provided by a submitter pursuant to this provision may itself be subject to disclosure under the FOIA.

(4) Decision and notice of intent to disclose.
(i) The Agency shall consider carefully a submitter's objections and specific grounds for nondisclosure prior to its final determination. If the Agency decides
to disclose a document over the objection of a submitter, the Agency shall provide the submitter a written notice which shall include:
(A) A statement of the reasons for which the submitter's disclosure objections were not sustained;
(B) A description of the information to be disclosed; and
(C) A specified disclosure date which is seven (7) days after the date of the instant notice.
(iii) When notice is given to a submitter under this section, the Agency shall also notify the requester and, if the Agency notifies a submitter that it intends to disclose information, then the requester shall be notified also and given the proposed date for disclosure.

(5) Notice of FOIA lawsuit.
If a requester initiates a civil action seeking to compel disclosure of information asserted to be within the scope of this section, the Agency shall promptly notify the submitter. The submitter, as specified above, shall provide such litigation assistance as required by the Agency and the Department of Justice.

(6) Exceptions to notice requirement.
The notice requirements of this section shall not apply if the Agency determines that:
(i) The information should not be disclosed in light of other FOIA exemptions;
(ii) The information has been published lawfully or has been officially made available to the public;
(iii) The disclosure of the information is otherwise required by law or federal regulation; or
(iv) The designation made by the submitter under this section appears frivolous, except that, in such a case, the Agency will, within a reasonable time prior to the specified disclosure date, give the submitter written notice of any final decision to disclose the information.

32 CFR Section 1900.32: Procedures for information concerning other persons.

(a) In general.

Personal information concerning individuals other than the requester shall not be disclosed under the Freedom of Information Act if the proposed release would constitute a clearly unwarranted invasion of personal privacy. See 5 U.S.C. 552(b)(6). For purposes of this section, the following definitions apply:

(1) Personal information
means any information about an individual that is not a matter of public record, or easily discernible to the public, or protected from disclosure because of the implications that arise from Government possession of such information.
(2) **Public interest**

means the public interest in understanding the operations and activities of the United States Government and not simply any matter which might be of general interest to the requester or members of the public.

(b) **Determination to be made.**

In making the required determination under this section and pursuant to exemption (b)(6) of the FOIA, the Agency will balance the privacy interests that would be compromised by disclosure against the public interest in release of the requested information.

(c) **Otherwise.**

A requester seeking information on a third person is encouraged to provide a signed affidavit or declaration from the third person waiving all or some of their privacy rights. However, all such waivers shall be narrowly construed and the Coordinator, in the exercise of his discretion and administrative authority, may seek clarification from the third party prior to any or all releases.

32 CFR Section 1900.33: Allocation of resources; agreed extensions of time.

(a) **In general.**

Agency components shall devote such personnel and other resources to the responsibilities imposed by the Freedom of Information Act as may be appropriate and reasonable considering:

1. The totality of resources available to the component,
2. The business demands imposed on the component by the Director of Central Intelligence or otherwise by law,
3. The information review and release demands imposed by the Congress or other governmental authority, and
4. The rights of all members of the public under the various information review and disclosure laws.

(b) **Discharge of FOIA responsibilities.**

Components shall exercise due diligence in their responsibilities under the FOIA and must allocate a reasonable level of resources to requests under the Act in a strictly “first-in, first-out” basis and utilizing two or more processing queues to ensure that smaller as well as larger (i.e., project) cases receive equitable attention. The Information and Privacy Coordinator is responsible for management of the Agency-wide program defined by this part and for establishing priorities for cases consistent with established law. The Director, Information Management through the Agency Release Panel shall provide policy
and resource direction as necessary and render decisions on administrative appeals.

(c) Requests for extension of time.

When the Agency is unable to meet the statutory time requirements of the FOIA, it will inform the requester that the request cannot be processed within the statutory time limits, provide an opportunity for the requester to limit the scope of the request so that it can be processed within the statutory time limits, or arrange with the requester an agreed upon time frame for processing the request, or determine that exceptional circumstances mandate additional time. In such instances the Agency will, however, inform a requester of his or her right to decline our request and proceed with an administrative appeal or judicial review as appropriate. Effective October 2, 1997, the definition of exceptional circumstances is modified per section 552(a)(6)(C) of the Freedom of Information Act, as amended.

32 CFR Section 1900.34: Requests for expedited processing.

(a) In general.

All requests will be handled in the order received on a strictly “first-in, first-out” basis. Exceptions to this rule will only be made in accordance with the following procedures. In all circumstances, however, and consistent with established judicial precedent, requests more properly the scope of requests under the Federal Rules of Civil or Criminal Procedure (or other federal, state, or foreign judicial or quasi-judicial rules) will not be granted expedited processing under this or related (e.g., Privacy Act) provisions unless expressly ordered by a federal court of competent jurisdiction.

(b) Procedure prior to October 2, 1997.

Requests for expedited processing shall be granted only in circumstances that the Agency deems to be exceptional. In making this determination, the Agency shall consider and must decide in the affirmative on all of the following factors:

(i) That there is a genuine need for the specific requested records; and
(ii) That the personal need is exceptional; and
(iii) That there are no alternative forums for the records or information sought; and
(iv) That it is reasonably believed that substantive records relevant to the stated needs may exist and be deemed releasable.

(2) In sum, requests shall be considered for expedited processing only when health, humanitarian, or due process considerations involving possible deprivation of life or liberty create circumstances of exceptional urgency and extraordinary need.
Requests for expedited processing will be approved only when a compelling need is established to the satisfaction of the Agency. A requester may make such a request with a certification of “compelling need” and, within ten (10) days of receipt, the Agency will decide whether to grant expedited processing and will notify the requester of its decision. The certification shall set forth with specificity the relevant facts upon which the requester relies and it appears to the Agency that substantive records relevant to the stated needs may exist and be deemed releasable. A “compelling need” is deemed to exist:

1. When the matter involves an imminent threat to the life or physical safety of an individual; or
2. When the request is made by a person primarily engaged in disseminating information and the information is relevant to a subject of public urgency concerning an actual or alleged Federal government activity.

CIA Action on FOIA Administrative Appeals

32 CFR Section 1900.41: Establishment of appeals structure.

(a) In general.

Two administrative entities have been established by the Director of Central Intelligence to facilitate the processing of administrative appeals under the Freedom of Information Act. Their membership, authority, and rules of procedure are as follows.

(b) Historical Records Policy Board (“HRPB” or “Board”).

This Board, the successor to the CIA Information Review Committee, acts as the senior corporate board in the CIA on all matters of information review and release.

(1) Membership.
The HRPB is composed of the Executive Director, who serves as its Chair, the Deputy Director for Administration, the Deputy Director for Intelligence, the Deputy Director for Operations, the Deputy Director for Science and Technology, the General Counsel, the Director of Congressional Affairs, the Director of the Public Affairs Staff, the Director, Center for the Study of Intelligence, and the Associate Deputy Director for Administration/Information Services, or their designees.

(2) Authorities and activities.
The HRPB, by majority vote, may delegate to one or more of its members the authority to act on any appeal or other matter or authorize the Chair to delegate such authority, as long as such delegation is not to the same individual or body who made the initial denial. The Executive Secretary of the HRPB is the Director,
Information Management. The Chair may request interested parties to participate when special equities or expertise are involved.

(c) Agency Release Panel (“ARP” or “Panel”).

The HRPB, pursuant to its delegation of authority, has established a subordinate Agency Release Panel.

(1) Membership.
The ARP is composed of the Director, Information Management, who serves as its Chair; the Information Review Officers from the Directorates of Administration, Intelligence, Operations, Science and Technology, and the Director of Central Intelligence Area; the CIA Information and Privacy Coordinator; the Chief, Historical Review Group; the Chair, Publications Review Board; the Chief, Records Declassification Program; and representatives from the Office of General Counsel, the Office of Congressional Affairs, and the Public Affairs Staff.

(2) Authorities and activities.
The Panel shall meet on a regular schedule and may take action when a simple majority of the total membership is present. The Panel shall advise and assist the HRPB on all information release issues, monitor the adequacy and timeliness of Agency releases, set component search and review priorities, review adequacy of resources available to and planning for all Agency release programs, and perform such other functions as deemed necessary by the Board. The Information and Privacy Coordinator also serves as Executive Secretary of the Panel. The Chair may request interested parties to participate when special equities or expertise are involved. The Panel, functioning as a committee of the whole or through individual members, will make final Agency decisions from appeals of initial adverse decisions under the Freedom of Information Act and such other information release decisions made under 32 CFR parts 1901, 1907, and 1908. Issues shall be decided by a majority of members present; in all cases of a divided vote, any member of the ARP then present may refer such matter to the HRPB by written memorandum to the Executive Secretary of the HRPB. Matters decided by the Panel or Board will be deemed a final decision by the Agency.

32 CFR Section 1900.42: Right of appeal and appeal procedures.

(a) Right of Appeal.

A right of administrative appeal exists whenever access to any requested record or any portion thereof is denied, no records are located in response to a request, or a request for a fee waiver is denied. The Agency will apprise all requesters in writing of their right to appeal such decisions to the CIA Agency Release Panel through the Coordinator.

(b) Requirements as to time and form.
Appeals of decisions must be received by the Coordinator within forty-five (45) days of the date of the Agency's initial decision. The Agency may, for good cause and as a matter of administrative discretion, permit an additional thirty (30) days for the submission of an appeal. All appeals shall be in writing and addressed as specified in 32 CFR 1900.03. All appeals must identify the documents or portions of documents at issue with specificity and may present such information, data, and argument in support as the requester may desire.

(c) Exceptions.

No appeal shall be accepted if the requester has outstanding fees for information services at this or another federal agency. In addition, no appeal shall be accepted if the information in question has been the subject of a review within the previous two (2) years or is the subject of pending litigation in the federal courts.

(d) Receipt, recording, and tasking.

The Agency shall promptly record each request received under this part, acknowledge receipt to the requester in writing, and thereafter effect the necessary taskings to the Deputy Director(s) in charge of the directorate(s) which originated or has an interest in the record(s) subject to the appeal. As used herein, the term Deputy Director includes an equivalent senior official in the DCI-area as well as a designee known as the Information Review Officer for a directorate or area.

(e) Time for response.

The Agency shall attempt to complete action on an appeal within twenty (20) days of the date of receipt. The current volume of requests, however, often requires that the Agency request additional time from the requester pursuant to 32 CFR 1900.33. In such event, the Agency will inform the requester of the right to judicial review.

32 CFR Section 1900.43: Determination(s) by Deputy Director(s).
Each Deputy Director in charge of a directorate which originated or has an interest in any of the records subject to the appeal, or designee, is a required party to any appeal; other interested parties may become involved through the request of the Coordinator when it is determined that some or all of the information is also within their official cognizance. These parties shall respond in writing to the Coordinator with a finding as to the exempt status of the information. This response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the parties and consistent with the information rights of members of the general public under the various information review and release laws.

32 CFR Section 1900.44: Action by appeals authority.
(a) Preparation of docket.

The Coordinator, acting in the capacity of Executive Secretary of the Agency Release Panel, shall place administrative appeals of FOIA requests ready for adjudication on the agenda at the next occurring meeting of that Panel. The Executive Secretary shall provide a summation memorandum for consideration of the members; the complete record of the request consisting of the request, the document(s) (sanitized and full text) at issue, and the findings of the concerned Deputy Director(s) or designee(s).

(b) Decision by the Agency Release Panel.

The Agency Release Panel shall meet and decide requests sitting as a committee of the whole. Decisions are by majority vote of those present at a meeting and shall be based on the written record and their deliberations; no personal appearances shall be permitted without the express permission of the Panel.

(c) Decision by the Historical Records Policy Board.

In any cases of divided vote by the ARP, any member of that body is authorized to refer the request to the CIA Historical Records Policy Board which acts as the senior corporate board for the Agency. The record compiled (the request, the memoranda filed by the originator and interested parties, and the previous decision(s)) as well as any memorandum of law or policy the referent desires to be considered, shall be certified by the Executive Secretary of the Agency Release Panel and shall constitute the official record of the proceedings and must be included in any subsequent filings.

32 CFR Section 1900.45: Notification of decision and right of judicial review.

The Executive Secretary of the Agency Release Panel shall promptly prepare and communicate the decision of the Panel or Board to the requester. With respect to any decision to deny information, that correspondence shall state the reasons for the decision, identify the officer responsible, and include a notice of a right to judicial review.
32 CFR PART 1901—PUBLIC RIGHTS UNDER THE PRIVACY ACT OF 1974

- General
  - 1901.01: Authority and purpose.
  - 1901.02: Definitions.
  - 1901.03: Contact for general information and requests.
  - 1901.04: Suggestions and complaints.
- Filing of Privacy Act Requests
  - 1901.11: Preliminary information.
  - 1901.12: Requirements as to form.
  - 1901.13: Requirements as to identification of requester.
  - 1901.14: Fees.
- Action on Privacy Act Requests
  - 1901.21: Processing requests for access to or amendment of records.
  - 1901.22: Action and determination(s) by originator(s) or any interested party.
  - 1901.23: Notification of decision and right of appeal.
- Additional Administrative Matters
  - 1901.31: Special procedures for medical and psychological records.
  - 1901.32: Requests for expedited processing.
  - 1901.33: Allocation of resources; agreed extensions of time.
- Action on Privacy Act Administrative Appeals
  - 1901.41: Establishment of appeals structure.
  - 1901.42: Right of appeal and appeal procedures.
  - 1901.43: Determination(s) by Deputy Director(s).
  - 1901.44: Action by appeals authority.
  - 1901.45: Notification of decision and right of judicial review.
- Prohibitions
  - 1901.51: Limitations on disclosure.
  - 1901.52: Criminal penalties.
- Exemptions
  - 1901.61: Purpose and authority.
  - 1901.62: General exemptions.
  - 1901.63: Specific exemptions.

Authority:
National Security Act of 1947, as amended; Central Intelligence Agency Act of 1949, as amended; Privacy Act, as amended; and Executive Order 12958 (or successor Orders).
Source:
62 FR 32488, June 16, 1997, unless otherwise noted.

General
32 CFR Section 1901.01: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement the Privacy Act of 1974 (5 U.S.C. 552a); sec. 102 of the National Security Act of 1947, as amended (50 U.S.C. 403); and sec. 6 of the Central Intelligence Agency Act of 1949, as amended (50 U.S.C. 403g).

(b) Purpose in general.

This part prescribes procedures for a requester, as defined herein:
(1) To request notification of whether the Central Intelligence Agency maintains a record concerning them in any non-exempt portion of a system of records or any non-exempt system of records;
(2) To request a copy of all non-exempt records or portions of records;
(3) To request that any such record be amended or augmented; and
(4) To file an administrative appeal to any initial adverse determination to deny access to or amend a record.

(c) Other purposes.

This part also sets forth detailed limitations on how and to whom the Agency may disclose personal information and gives notice that certain actions by officers or employees of the United States Government or members of the public could constitute criminal offenses.

32 CFR Section 1901.02: Definitions.
For purposes of this part, the following terms have the meanings indicated:

(a) Agency or CIA

means the United States Central Intelligence Agency acting through the CIA Information and Privacy Coordinator;

(b) Days

means calendar days when the Agency is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

(c) Control
means ownership or the authority of the CIA pursuant to federal statute or privilege to regulate official or public access to records;

(d) Coordinator

means the CIA Information and Privacy Coordinator who serves as the Agency manager of the information review and release program instituted under the Privacy Act;

(e) Federal agency

means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

(f) Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of the CIA, has a subject matter or physical interest in the documents or information at issue;

(g) Maintain

means maintain, collect, use, or disseminate;

(h) Originator

means the U.S. Government official who originated the document at issue or successor in office or such official who has been delegated release or declassification authority pursuant to law;

(i) Privacy Act or PA

means the statute as codified at 5 U.S.C. 552a;

(j) Record

means an item, collection, or grouping of information about an individual that is maintained by the Central Intelligence Agency in a system of records;

(k) Requester or individual

means a citizen of the United States or an alien lawfully admitted for permanent residence who is a living being and to whom a record might pertain;

(l) Responsive record

means those documents (records) which the Agency has determined to be within the scope of a Privacy Act request;
(m) Routine use

means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which the record is maintained;

(n) System of records

means a group of any records under the control of the Central Intelligence Agency from which records are retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to that individual.

32 CFR Section 1901.03: Contact for general information and requests.

For general information on this part, to inquire about the Privacy Act program at CIA, or to file a Privacy Act request, please direct your communication in writing to the Information and Privacy Coordinator, Central Intelligence Agency, Washington, DC. 20505. Requests with the required identification statement pursuant to 32 CFR 1901.13 must be filed in original form by mail. Subsequent communications and any inquiries will be accepted by mail or facsimile at (703) 613-3007 or by telephone at (703) 613-1287. Collect calls cannot be accepted.

32 CFR Section 1901.04: Suggestions and complaints.

The Agency welcomes suggestions or complaints with regard to its administration of the Privacy Act. Many requesters will receive pre-paid, customer satisfaction survey cards. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. The Agency will respond to all substantive communications and take such actions as determined feasible and appropriate.

Filing of Privacy Act Requests

32 CFR Section 1901.11: Preliminary information.

Members of the public shall address all communications to the contact specified at § 1901.03 and clearly delineate the communication as a request under the Privacy Act and this regulation. Requests and administrative appeals on requests, referrals, and coordinations received from members of the public who owe outstanding fees for information services at this or other federal agencies will not be accepted and action on existing requests and appeals will be terminated in such circumstances.

32 CFR Section 1901.12: Requirements as to form.

(a) In general.

No particular form is required. All requests must contain the identification information required at § 1901.13.
(b) For access.

For requests seeking access, a requester should, to the extent possible, describe the nature of the record sought and the record system(s) in which it is thought to be included. Requesters may find assistance from information described in the Privacy Act Issuances Compilation which is published biannually by the Federal Register. In lieu of this, a requester may simply describe why and under what circumstances it is believed that this Agency maintains responsive records; the Agency will undertake the appropriate searches.

(c) For amendment.

For requests seeking amendment, a requester should identify the particular record or portion subject to the request, state a justification for such amendment, and provide the desired amending language.

32 CFR Section 1901.13: Requirements as to identification of requester.

(a) In general.

Individuals seeking access to or amendment of records concerning themselves shall provide their full (legal) name, address, date and place of birth, and current citizenship status together with a statement that such information is true under penalty of perjury or a notarized statement swearing to or affirming identity. If the Agency determines that this information is not sufficient, the Agency may request additional or clarifying information.

(b) Requirement for aliens.

Only aliens lawfully admitted for permanent residence (PRAs) may file a request pursuant to the Privacy Act and this part. Such individuals shall provide, in addition to the information required under paragraph (a) of this section, their Alien Registration Number and the date that status was acquired.

(c) Requirement for representatives.

The parent or guardian of a minor individual, the guardian of an individual under judicial disability, or an attorney retained to represent an individual shall provide, in addition to establishing the identity of the minor or individual represented as required in paragraph (a) or (b) of this section, evidence of such representation by submission of a certified copy of the minor's birth certificate, court order, or representational agreement which establishes the relationship and the requester's identity.

(d) Procedure otherwise.
If a requester or representative fails to provide the information in paragraph (a), (b), or (c) of this section within forty-five (45) days of the date of our request, the Agency will deem the request closed. This action, of course, would not prevent an individual from refiling his or her Privacy Act request at a subsequent date with the required information.

32 CFR Section 1901.14: Fees.
No fees will be charged for any action under the authority of the Privacy Act, 5 U.S.C. 552a, irrespective of the fact that a request is or may be processed under the authority of both the Privacy Act and the Freedom of Information Act.

Action on Privacy Act Requests

32 CFR Section 1901.21: Processing requests for access to or amendment of records.

(a) In general.

Requests meeting the requirements of 32 CFR 1901.11 through 1901.13 shall be processed under both the Freedom of Information Act, 5 U.S.C. 552, and the Privacy Act, 5 U.S.C. 552a, and the applicable regulations, unless the requester demands otherwise in writing. Such requests will be processed under both Acts regardless of whether the requester cites one Act in the request, both, or neither. This action is taken in order to ensure the maximum possible disclosure to the requester.

(b) Receipt, recording and tasking.

Upon receipt of a request meeting the requirements of §§ 1901.11 through 1901.13, the Agency shall within ten (10) days record each request, acknowledge receipt to the requester, and thereafter effect the necessary taskings to the components reasonably believed to hold responsive records.

(c) Effect of certain exemptions.

In processing a request, the Agency shall decline to confirm or deny the existence or nonexistence of any responsive records whenever the fact of their existence or nonexistence is itself classified under Executive Order 12958 or revealing of intelligence sources and methods protected pursuant to section 103(c)(5) of the National Security Act of 1947. In such circumstances, the Agency, in the form of a final written response, shall so inform the requester and advise of his or her right to an administrative appeal.

(d) Time for response.

Although the Privacy Act does not mandate a time for response, our joint treatment of requests under both the Privacy Act and the FOIA means that the
Agency should provide a response within the FOIA statutory guideline of ten (10) days on initial requests and twenty (20) days on administrative appeals. However, the current volume of requests require that the Agency often seek additional time from a requester pursuant to 32 CFR 1901.33. In such event, the Agency will inform the requester in writing and further advise of his or her right to file an administrative appeal.

32 CFR Section 1901.22: Action and determination(s) by originator(s) or any interested party.

(a) Initial action for access.

CIA components tasked pursuant to a Privacy Act access request shall search all relevant record systems within their cognizance. They shall:

(1) Determine whether responsive records exist;
(2) Determine whether access must be denied in whole or part and on what legal basis under both Acts in each such case;
(3) Approve the disclosure of records for which they are the originator; and
(4) Forward to the Coordinator all records approved for release or necessary for coordination with or referral to another originator or interested party as well as the specific determinations with respect to denials (if any).

(b) Initial action for amendment.

CIA components tasked pursuant to a Privacy Act amendment request shall review the official records alleged to be inaccurate and the proposed amendment submitted by the requester. If they determine that the Agency’s records are not accurate, relevant, timely or complete, they shall promptly:

(1) Make the amendment as requested;
(2) Write to all other identified persons or agencies to whom the record has been disclosed (if an accounting of the disclosure was made) and inform of the amendment; and
(3) Inform the Coordinator of such decisions.

(c) Action otherwise on amendment request.

If the CIA component records manager declines to make the requested amendment or declines to make the requested amendment but agrees to augment the official records, that manager shall promptly:

(1) Set forth the reasons for refusal; and
(2) Inform the Coordinator of such decision and the reasons therefore.

(d) Referrals and coordinations.

As applicable and within ten (10) days of receipt by the Coordinator, any CIA records containing information originated by other CIA components shall be
forwarded to those entities for action in accordance with paragraphs (a), (b), or (c) of this section and return. Records originated by other federal agencies or CIA records containing other federal agency information shall be forwarded to such agencies within ten (10) days of our completion of initial action in the case for action under their regulations and direct response to the requester (for other agency records) or return to the CIA (for CIA records).

(e) Effect of certain exemptions.

This section shall not be construed to allow access to systems of records exempted by the Director of Central Intelligence pursuant to subsections (j) and (k) of the Privacy Act or where those exemptions require that the CIA can neither confirm nor deny the existence or nonexistence of responsive records.

32 CFR Section 1901.23: Notification of decision and right of appeal.
Within ten (10) days of receipt of responses to all initial taskings and subsequent coordinations (if any), and dispatch of referrals (if any), the Agency will provide disclosable records to the requester. If a determination has been made not to provide access to requested records (in light of specific exemptions) or that no records are found, the Agency shall so inform the requester, identify the denying official, and advise of the right to administrative appeal.

Additional Administrative Matters

32 CFR Section 1901.31: Special procedures for medical and psychological records.

(a) In general.

When a request for access or amendment involves medical or psychological records and when the originator determines that such records are not exempt from disclosure, the Agency will, after consultation with the Director of Medical Services, determine:
(1) Which records may be sent directly to the requester and
(2) Which records should not be sent directly to the requester because of possible medical or psychological harm to the requester or another person.

(b) Procedure for records to be sent to physician.

In the event that the Agency determines, in accordance with paragraph (a)(2) of this section, that records should not be sent directly to the requester, the Agency will notify the requester in writing and advise that the records at issue can be made available only to a physician of the requester's designation. Upon receipt of such designation, verification of the identity of the physician, and agreement by the physician:
(1) To review the documents with the requesting individual,
(2) To explain the meaning of the documents, and
(3) To offer counseling designed to temper any adverse reaction, the Agency will forward such records to the designated physician.

(c) Procedure if physician option not available.

If within sixty (60) days of the paragraph (a)(2) of this section, the requester has failed to respond or designate a physician, or the physician fails to agree to the release conditions, the Agency will hold the documents in abeyance and advise the requester that this action may be construed as a technical denial. The Agency will also advise the requester of the responsible official and of his or her rights to administrative appeal and thereafter judicial review.

32 CFR Section 1901.32: Requests for expedited processing.
(a) All requests will be handled in the order received on a strictly “first-in, first-out” basis. Exceptions to this rule will only be made in circumstances that the Agency deems to be exceptional. In making this determination, the Agency shall consider and must decide in the affirmative on all of the following factors:
(1) That there is a genuine need for the records; and
(2) That the personal need is exceptional; and
(3) That there are no alternative forums for the records sought; and
(4) That it is reasonably believed that substantive records relevant to the stated needs may exist and be deemed releasable.
(b) In sum, requests shall be considered for expedited processing only when health, humanitarian, or due process considerations involving possible deprivation of life or liberty create circumstances of exceptional urgency and extraordinary need. In accordance with established judicial precedent, requests more properly the scope of requests under the Federal Rules of Civil or Criminal Procedure (or equivalent state rules) will not be granted expedited processing under this or related (e.g., Freedom of Information Act) provisions unless expressly ordered by a federal court of competent jurisdiction.

32 CFR Section 1901.33: Allocation of resources; agreed extensions of time.
(a) In general.

Agency components shall devote such personnel and other resources to the responsibilities imposed by the Privacy Act as may be appropriate and reasonable considering:
(1) The totality of resources available to the component,
(2) The business demands imposed on the component by the Director of Central Intelligence or otherwise by law,
(3) The information review and release demands imposed by the Congress or other governmental authority, and
(4) The rights of all members of the public under the various information review and disclosure laws.

(b) Discharge of Privacy Act responsibilities.

Components shall exercise due diligence in their responsibilities under the Privacy Act and must allocate a reasonable level of resources to requests under the Act in a strictly “first-in, first-out” basis and utilizing two or more processing queues to ensure that smaller as well as larger (i.e., project) cases receive equitable attention. The Information and Privacy Coordinator is responsible for management of the Agency-wide program defined by this part and for establishing priorities for cases consistent with established law. The Director, Information Management through the Agency Release Panel shall provide policy and resource direction as necessary and shall make determinations on administrative appeals.

(c) Requests for extension of time.

While the Privacy Act does not specify time requirements, our joint treatment of requests under the FOIA means that when the Agency is unable to meet the statutory time requirements of the FOIA, the Agency may request additional time from a requester. In such instances the Agency will inform a requester of his or her right to decline our request and proceed with an administrative appeal or judicial review as appropriate.

Action on Privacy Act Administrative Appeals

32 CFR Section 1901.41: Establishment of appeals structure.

(a) In general.

Two administrative entities have been established by the Director of Central Intelligence to facilitate the processing of administrative appeals under the Freedom of Information Act. Their membership, authority, and rules of procedure are as follows.

(b) Historical Records Policy Board (“HRPB” or “Board”).

This Board, the successor to the CIA Information Review Committee, acts as the senior corporate board in the CIA on all matters of information review and release.

(1) Membership.
The HRPB is composed of the Executive Director, who serves as its Chair, the Deputy Director for Administration, the Deputy Director for Intelligence, the Deputy Director for Operations, the Deputy Director for Science and Technology, the General Counsel, the Director of Congressional Affairs, the Director of the
Public Affairs Staff, the Director, Center for the Study of Intelligence, and the Associate Deputy Director for Administration/Information Services, or their designees.

(2) Authorities and activities.
The HRPB, by majority vote, may delegate to one or more of its members the authority to act on any appeal or other matter or authorize the Chair to delegate such authority, as long as such delegation is not to the same individual or body who made the initial denial. The Executive Secretary of the HRPB is the Director, Information Management. The Chair may request interested parties to participate when special equities or expertise are involved.

(e) Agency Release Panel (“ARP” or “Panel”).

The HRPB, pursuant to its delegation of authority, has established a subordinate Agency Release Panel.

(1) Membership.
The ARP is composed of the Director, Information Management, who serves as its Chair; the Information Review Officers from the Directorates of Administration, Intelligence, Operations, Science and Technology, and the Director of Central Intelligence Area; the CIA Information and Privacy Coordinator; the Chief, Historical Review Group; the Chair, Publications Review Board; the Chief, Records Declassification Program; and representatives from the Office of General Counsel, the Office of Congressional Affairs, and the Public Affairs Staff.

(2) Authorities and activities.
The Panel shall meet on a regular schedule and may take action when a simple majority of the total membership is present. The Panel shall advise and assist the HRPB on all information release issues, monitor the adequacy and timeliness of Agency releases, set component search and review priorities, review adequacy of resources available to and planning for all Agency release programs, and perform such other functions as deemed necessary by the Board. The Information and Privacy Coordinator also serves as Executive Secretary of the Panel. The Chair may request interested parties to participate when special equities or expertise are involved. The Panel, functioning as a committee of the whole or through individual members, will make final Agency decisions from appeals of initial adverse decisions under the Freedom of Information Act and such other information release decisions made under 32 CFR parts 1901, 1907, and 1908. Issues shall be decided by a majority of members present; in all cases of a divided vote, any member of the ARP then present may refer such matter to the HRPB by written memorandum to the Executive Secretary of the HRPB. Matters decided by the Panel or Board will be deemed a final decision by the Agency.

32 CFR Section 1901.42: Right of appeal and appeal procedures.
(a) Right of Appeal.

A right of administrative appeal exists whenever access to any requested record or any portion thereof is denied, no records are located in response to a request, or a request for amendment is denied. The Agency will apprise all requesters in writing of their right to appeal such decisions to the CIA Agency Release Panel through the Coordinator.

(b) Requirements as to time and form.

Appeals of decisions must be received by the Coordinator within forty-five (45) days of the date of the Agency's initial decision. The Agency may, for good cause and as a matter of administrative discretion, permit an additional thirty (30) days for the submission of an appeal. All appeals to the Panel shall be in writing and addressed as specified in 32 CFR 1901.03. All appeals must identify the documents or portions of documents at issue with specificity, provide the desired amending language (if applicable), and may present such information, data, and argument in support as the requester may desire.

(c) Exceptions.

No appeal shall be accepted if the requester has outstanding fees for information services at this or another federal agency. In addition, no appeal shall be accepted if the information in question has been the subject of an administrative review within the previous two (2) years or is the subject of pending litigation in the federal courts.

(d) Receipt, recording, and tasking.

The Agency shall promptly record each administrative appeal, acknowledge receipt to the requester in writing, and thereafter effect the necessary taskings to the Deputy Director(s) in charge of the directorate(s) which originated or has an interest in the record(s) subject to the appeal. As used herein, the term Deputy Director includes an equivalent senior official within the DCI-area as well as a designee known as the Information Review Officer for a directorate or area.

32 CFR Section 1901.43: Determination(s) by Deputy Director(s).

Each Deputy Director in charge of a directorate which originated or has an interest in any of the records subject to the appeal, or designee, is a required party to any appeal; other interested parties may become involved through the request of the Coordinator when it is determined that some or all of the information is also within their official cognizance. These parties shall respond in writing to the Coordinator with a finding as to the exempt or non-exempt status of the information including citations to the applicable exemption and/or their agreement or disagreement as to the requested amendment and the reasons therefore. Each response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the parties and consistent
with the information rights of members of the general public under the various
information review and release laws.

32 CFR Section 1901.44: Action by appeals authority.

(a) Preparation of docket.

The Coordinator, acting as the Executive Secretary of the Agency Release Panel,
shall place administrative appeals of Privacy Act requests ready for adjudication
on the agenda at the next occurring meeting of that Panel. The Executive
Secretary shall provide a summation memorandum for consideration of the
members; the complete record of the request consisting of the request, the
document(s) (sanitized and full text) at issue, and the findings of the concerned
Deputy Director(s) or designee(s).

(b) Decision by the Agency Release Panel.

The Agency Release Panel shall meet and decide requests sitting as a committee
of the whole. Decisions are by majority vote of those present at a meeting and
shall be based on the written record and their deliberations; no personal
appearances shall be permitted without the express permission of the Panel.

(c) Decision by the Historical Records Policy Board.

In any cases of divided vote by the ARP, any member of that body is authorized
to refer the request to the CIA Historical Records Policy Board which acts as the
senior corporate board for the Agency. The record compiled (the request, the
memoranda filed by the originator and interested parties, and the previous
decision(s)) as well as any memorandum of law or policy the referent desires to
be considered, shall be certified by the Executive Secretary of the Agency Release
Panel and shall constitute the official record of the proceedings and must be
included in any subsequent filings.

32 CFR Section 1901.45: Notification of decision and right of
judicial review.

(a) In general.

The Executive Secretary of the Agency Release Panel shall promptly prepare and
communicate the decision of the Panel or Board to the requester. With respect to
any decision to deny information or deny amendment, that correspondence shall
state the reasons for the decision, identify the officer responsible, and include a
notice of the right to judicial review.

(b) For amendment requests.
With further respect to any decision to deny an amendment, that correspondence shall also inform the requester of the right to submit within forty-five (45) days a statement of his or her choice which shall be included in the official records of the CIA. In such cases, the applicable record system manager shall clearly note any portion of the official record which is disputed, append the requester's statement, and provide copies of the statement to previous recipients (if any are known) and to any future recipients when and if the disputed information is disseminated in accordance with a routine use.

Prohibitions

32 CFR Section 1901.51: Limitations on disclosure.

No record which is within a system of records shall be disclosed by any means of communication to any individual or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be:

(a) To those officers and employees of this Agency which maintains the record who have a need for the record in the performance of their duties;
(b) Required under the Freedom of Information Act, 5 U.S.C. 552;
(c) For a routine use as defined in § 1901.02(m), as contained in the Privacy Act Issuances Compilation which is published biennially in the Federal Register, and as described in §§ (a)(7) and (e)(4)(D) of the Act;
(d) To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of U.S.C. Title 13;
(e) To a recipient who has provided the Agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
(f) To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or designee to determine whether the record has such value;
(g) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of that agency or instrumentality has made a written request to the CIA specifying the particular information desired and the law enforcement activity for which the record is sought;
(h) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
(i) To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
(j) To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office; or
(k) To any agency, government instrumentality, or other person or entity pursuant to the order of a court of competent jurisdiction of the United States or constituent states.

32 CFR Section 1901.52: Criminal penalties.

(a) Unauthorized disclosure.

Criminal penalties may be imposed against any officer or employee of the CIA who, by virtue of employment, has possession of or access to Agency records which contain information identifiable with an individual, the disclosure of which is prohibited by the Privacy Act or by these rules, and who, knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive same.

(b) Unauthorized maintenance.

Criminal penalties may be imposed against any officer or employee of the CIA who willfully maintains a system of records without meeting the requirements of section (e)(4) of the Privacy Act, 5 U.S.C.552a. The Coordinator and the Inspector General are authorized independently to conduct such surveys and inspect such records as necessary from time to time to ensure that these requirements are met.

(c) Unauthorized requests.

Criminal penalties may be imposed upon any person who knowingly and willfully requests or obtains any record concerning an individual from the CIA under false pretenses.

Exemptions
32 CFR Section 1901.61: Purpose and authority.

Purpose of exemptions.

This part sets forth those systems of records or portions of systems of records which the Director of Central Intelligence has determined to exempt from the procedures established by this regulation and from certain provisions of the Privacy Act:

(a) The purpose of the following specified general exemption of polygraph records is to prevent access and review of records which intimately reveal CIA operational methods. The purpose of the general exemption from the provisions of sections (c)(3) and (e)(3) (A)-(D) of the Privacy Act is to avoid disclosures that may adversely affect ongoing operational relationships with other intelligence and related organizations and thus reveal or jeopardize intelligence sources and methods or risk exposure of intelligence sources and methods in the processing of covert employment applications.
(b) The purpose of the general exemption from sections (d), (e)(4)(G), (f)(1), and (g) of the Privacy Act is to protect only those portions of systems of records which if revealed would risk exposure of intelligence sources and methods or hamper the ability of the CIA to effectively use information received from other agencies or foreign governments.

(c) It should be noted that by subjecting information which would consist of, reveal, or pertain to intelligence sources and methods to separate determinations by the Director of Central Intelligence under the provision entitled “General exemptions,” 32 CFR 1901.62 regarding access and notice, an intent is established to apply the exemption from access and notice only in those cases where notice in itself would constitute a revelation of intelligence sources and methods; in all cases where only access to information would reveal such source or method, notice will be given upon request.

(d) The purpose of the general exemption for records that consist of, pertain to, or would otherwise reveal the identities of employees who provide information to the Office of the Inspector General is to implement section 17 of the CIA Act of 1949, as amended, 50 U.S.C. 403q(e)(3), and to ensure that no action constituting a reprisal or threat of reprisal is taken because an employee has cooperated with the Office of Inspector General.

(e) The purpose of the specific exemptions provided for under section (k) of the Privacy Act is to exempt only those portions of systems of records which would consist of, reveal, or pertain to that information which is enumerated in that section of the Act.

(f) In each case, the Director of Central Intelligence currently or then in office has determined that the enumerated classes of information should be exempt in order to comply with dealing with the proper classification of national defense or foreign policy information; protect the identification of persons who provide information to the CIA Inspector General; protect the privacy of other persons who supplied information under an implied or express grant of confidentiality in the case of law enforcement or employment and security suitability investigations (or promotion material in the case of the armed services); protect information used in connection with protective services under 18 U.S.C. 3056; protect the efficacy of testing materials; and protect information which is required by statute to be maintained and used solely as statistical records.

32 CFR Section 1901.62: General exemptions.

(a) Pursuant to authority granted in section (j) of the Privacy Act, the Director of Central Intelligence has determined to exempt from all sections of the Act—except sections 552a(b); (c) (1) and (2); (e) (1), (4) (A)–(F), (5), (6), (7), (9), (10), and (11); and (i)—the following systems of records or portions of records in a system of record:

(1) Polygraph records.
(2) [Reserved]

(b) Pursuant to authority granted in section (j) of the Privacy Act, the Director of Central Intelligence has determined to exempt from sections (e)(3) and (e)(3) (A)–(D) of the Act all systems of records maintained by this Agency.
(c) Pursuant to authority granted in section (j) of the Privacy Act, the Director of Central Intelligence has determined to exempt from notification under sections (e)(4)(G) and (f)(1) those portions of each and all systems of records which have been exempted from individual access under section (j) in those cases where the Coordinator determines after advice by the responsible components that confirmation of the existence of a record may jeopardize intelligence sources and methods. In such cases the Agency must neither confirm nor deny the existence of the record and will advise a requester that there is no record which is available pursuant to the Privacy Act of 1974.

(d) Pursuant to authority granted in section (j) of the Privacy Act, the Director of Central Intelligence has determined to exempt from access by individuals under section (d) of the Act those portions and only those portions of all systems of records maintained by the CIA that:

(1) Consist of, pertain to, or would otherwise reveal intelligence sources and methods;
(2) Consist of documents or information provided by any foreign government entity, international organization, or, any United States federal, state, or other public agency or authority; and
(3) Consist of information which would reveal the identification of persons who provide information to the CIA Inspector General.

(e) Pursuant to authority granted in section (j) of the Privacy Act, the Director of Central Intelligence has determined to exempt from judicial review under section (g) of the Act all determinations to deny access under section (d) of the Act and all decisions to deny notice under sections (e)(4)(G) and (f)(1) of the Act pursuant to determination made under paragraph (c) of this section when it has been determined by an appropriate official of the CIA that such access would disclose information which would:

(1) Consist of, pertain to, or otherwise reveal intelligence sources and methods;
(2) Consist of documents or information provided by any foreign government entity, international organization, or, any United States federal, state, or other public agency or authority; and
(3) Consist of information which would reveal the identification of persons who provide information to the CIA Inspector General.

32 CFR Section 1901.63: Specific exemptions.
Pursuant to authority granted in section (k) of the Privacy Act, the Director of Central Intelligence has determined to exempt from section (d) of the Privacy Act those portions and only those portions of all systems of records maintained by the CIA that would consist of, pertain to, or otherwise reveal information that is:

(a) Classified pursuant to Executive Order 12958 (or successor or prior Order) and thus subject to the provisions of 5 U.S.C. 552(b)(1) and 5 U.S.C. 552a(k)(1);
(b) Investigatory in nature and compiled for law enforcement purposes, other than material within the scope of section (j)(2) of the Act; provided however, that if an individual is denied any right, privilege, or benefit to which they are otherwise eligible, as a result of the maintenance of such material, then such material shall be provided to that individual except to the extent that the
disclosure would reveal the identity of a source who furnished the information to the United States Government under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;
(c) Maintained in connection with providing protective services to the President of the United States or other individuals pursuant to 18 U.S.C. 3056;
(d) Required by statute to be maintained and used solely as statistical records;
(e) Investigatory in nature and compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the United States Government under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;
(f) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or
(g) Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the United States Government under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality.
32 CFR Section 1902.13: Declassification and downgrading policy.

(a)-(b) [Reserved]

(c) The Executive Order provides that in some cases the need to protect properly classified information “may be outweighed by the public interest in disclosure of the information,” and that “when such questions arise” the competing interests in protection and disclosure are to be balanced. The Order further provides that the information is to be declassified in such cases if the balance is struck in favor of disclosure. The drafters of the Order recognized that such cases would be rare and that declassification decisions in such cases would remain the responsibility of the Executive Branch. For purposes of these provisions, a question as to whether the public interest favoring the continued protection of properly classified information is outweighed by a public interest in the disclosure of that information will be deemed to exist only in circumstances where, in the judgment of the agency, nondisclosure could reasonably be expected to:

1. Place a person’s life in jeopardy.
2. Adversely affect the public health and safety.
3. Impede legitimate law enforcement functions.
4. Impede the investigative or oversight functions of the Congress.
5. Obstruct the fair administration of justice.
6. Deprive the public of information indispensable to public decisions on issues of critical national importance (effective for declassification reviews conducted on or after 1 February 1980).

(d) When a case arises that requires a balancing of interests under paragraph (c) above, the reviewing official shall refer the matter to an Agency official having Top Secret classification authority, who shall balance. If it appears that the public interest in disclosure of the information may outweigh any continuing need for its protection, the case shall be referred with a recommendation for decision to the appropriate Deputy Director or Head of Independent Office. If those officials believe disclosure may be warranted, they, in coordination with OGC, as appropriate, shall refer the matter and a recommendation to the DDCI. If the DDCI determines that the public interest in disclosure of the information outweighs any damage to national security that might reasonably be expected to result from disclosure, the information shall be declassified.

[45 FR 64175, Sept. 29, 1980]
1903.1: Definitions.
1903.2: Applicability.
1903.3: State law applicable.
1903.4: Vehicles and traffic safety.
1903.5: Enforcement of parking regulations.
1903.6: Admission on to an Agency installation.
1903.7: Trespassing.
1903.8: Interfering with Agency functions.
1903.9: Explosives.
1903.10: Weapons.
1903.11: Restrictions on photographic, transmitting, and recording equipment.
1903.12: Alcoholic beverages and controlled substances.
1903.13: Intoxicated on an Agency installation.
1903.14: Disorderly conduct.
1903.15: Preservation of property.
1903.16: Restrictions on animals.
1903.17: Soliciting, vending, and debt collection.
1903.18: Distribution of materials.
1903.19: Gambling.
1903.20: Penalties and effects on other laws.

Authority:

Source:
63 FR 44786, Aug. 21, 1998, unless otherwise noted.
32 CFR Section 1903.1: Definitions.
As used in this part:

Agency installation.

For the purposes of this part, the term Agency installation means the property within the Agency Headquarters Compound and the property controlled and occupied by the Federal Highway Administration located immediately adjacent to such Compound, and property within any other Agency installation and protected property (i.e., property owned, leased, or otherwise controlled by the Central Intelligence Agency).

Authorized person.

An officer of the Security Protective Service, or any other Central Intelligence Agency employee who has been authorized by the Director of Central Intelligence pursuant to section 15 of the Central Intelligence Agency Act of 1949 to enforce the provisions of this part.

Blasting agents.

The term is defined for the purposes of this part as it is defined in Title 18 U.S.C. 841.

Controlled Substance.

Any drug or other substance, or immediate precursor that has been defined as a controlled substance in the Controlled Substances Act (Title 21 U.S.C. 801 et seq.).

Explosives/Explosive Materials.

The term is defined for the purposes of this part as it is defined in Title 18 U.S.C. 841.

Operator.

A person who operates, drives, controls, or otherwise has charge of, or is in actual physical control of a mechanical mode of transportation or any other mechanical equipment.
Permit.

A written authorization to engage in uses or activities that are otherwise prohibited, restricted, or regulated.

Possession.

Exercising direct physical control or dominion, with or without ownership, over the property.

State law.

The applicable and non-conflicting laws, statutes, regulations, ordinances, and codes of the State(s) and other political subdivision(s) within whose exterior boundaries an Agency installation or a portion thereof is located.

Traffic.

Pedestrians, ridden or herded animals, vehicles, and other conveyances, either singly or together, while using any road, path, street, or other thoroughfare for the purpose of travel.

Vehicles.

Any vehicle that is self-propelled or designed for self-propulsion, any motorized vehicle, and any vehicle drawn by or designed to be drawn by a motor vehicle, including any device in, upon, or by which any person or property is or can be transported or drawn upon a roadway, highway, hallway, or pathway; to include any device moved by human or animal power. Whether required to be licensed in any State or otherwise.

Weapons.

Any firearms or any other loaded or unloaded pistol, rifle, shotgun, or other weapon which is designed to, or may be readily converted to expel a projectile by ignition of a propellant, by compressed gas, or which is spring-powered. Any bow and arrow, crossbow, blowgun, spear gun, hand-thrown spear, sling-shot, irritant gas device, explosive device, or any other implement designed to discharge missiles; or a weapon, device, instrument, material, or substance, animate or inanimate, that is used for or is readily capable of, causing death or serious bodily injury, including any weapon the possession of which is prohibited under the laws of the State in which the Agency installation or portion thereof is located;
except that such term does not include a closing pocket knife with a blade of less than 2 1/2 inches in length.

32 CFR Section 1903.2: Applicability.
The provisions of this part apply to all Agency installations, and to all persons entering on to or when on an Agency installation. They supplement the provisions of Title 18, United States Code, relating to crimes and criminal procedures, and those provisions of State law that are federal criminal offenses by virtue of the Assimilative Crimes Act, 18 U.S.C. 13. The Director of Central Intelligence, at his discretion, may suspend the applicability of this part, or a portion thereof, on any Agency installation, or any portion of the installation, covered under this part. Where necessary and when consistent with national security requirements notices will be posted on the affected Agency installation to indicate that the applicability of this part or a portion thereof has been suspended.

32 CFR Section 1903.3: State law applicable.
(a) Unless specifically addressed by the regulations in this part, traffic safety and the permissible use and operation of vehicles within an Agency installation are governed by State law. State law that is now or may later be in effect is adopted and made a part of the regulations in this part.
(b) Violating a provision of State law is prohibited.

32 CFR Section 1903.4: Vehicles and traffic safety.

(a) Open container of alcoholic beverage.

(1) Each person within the vehicle is responsible for complying with the provisions of this section that pertain to carrying an open container. The operator of the vehicle is the person responsible for complying with the provisions of this section that pertain to the storage of an open container.
(2) Carrying or storing a bottle, can, or other receptacle containing an alcoholic beverage that is open or has been opened, or whose seal is broken, or the contents of which have been partially removed, within a vehicle on an Agency installation is prohibited.
(3) This section does not apply to:
(i) An open container stored in the trunk of a vehicle or, if a vehicle is not equipped with a trunk, to an open container stored in some other portion of the vehicle designated for the storage of luggage and not normally occupied by or readily accessible to the operator or passenger; or
(ii) An open container stored in the living quarters of a motor home or camper.
(4) For the purpose of paragraph (a)(3)(i) of this section, a utility compartment or glove compartment is deemed to be readily accessible to the operator and passengers of a vehicle.
(b) Operating under the influence of alcohol, drugs, or controlled substances.

(1) Operating or being in actual physical control of a vehicle is prohibited while:
(i) Under the influence of alcohol, drug or drugs, a controlled substance, or any combination thereof, to a degree that renders the operator incapable of safe operation; or
(ii) The alcohol concentration in the operator's blood is 0.08 grams or more of alcohol per 100 milliliters of blood or 0.08 grams or more alcohol per 210 liters of breath. Provided, however, that if the applicable State law that applies to operating a vehicle while under the influence of alcohol establishes more restrictive limits of alcohol concentration in the operator's blood or breath, those limits supersede the limits specified in this section.

(2) The provisions or paragraph (b)(1) of this section shall also apply to an operator who is or has been legally entitled to use alcohol or another drug.

(3) Test.
(i) At the request or direction of an authorized person who has probable cause to believe that an operator of a vehicle within an Agency installation has violated a provision of paragraph (b)(1) of this section, the operator shall submit to one or more tests of blood, breath, saliva, or urine for the purpose of determining blood alcohol, drug, and controlled substance content.
(ii) Refusal by an operator to submit to a test is prohibited and may result in detention and citation by an authorized person. Proof of refusal many be admissible in any related judicial proceeding.
(iii) Any test or tests for the presence of alcohol, drugs, and controlled substances shall be determined by and administered at the direction of an officer of the Security Protective Service.
(iv) Any test shall be conducted by using accepted scientific methods and equipment of proven accuracy and reliability and operated by personnel certified in its use.

(4) Presumptive levels.
(i) The results of chemical or other quantitative tests are intended to supplement the elements of probable cause used as the basis for the arrest of an operator charged with a violation of this section. If the alcohol concentration in the operator's blood or breath at the time of the testing is less than the alcohol concentration specified in paragraph (b)(1)(ii) of this section this fact does not give rise to any presumption that the operator is or is not under the influence of alcohol.
(ii) The provisions of paragraph (b)(4)(i) of this section are not intended to limit the introduction of any other competent evidence bearing upon the question of whether the operator, at the time of the alleged violation, was under the influence of alcohol, a drug or drugs, or a controlled substance, or any combination thereof.

[63 FR 44786, Aug. 21, 1998; 64 FR 27041, May 18, 1999]

32 CFR Section 1903.5: Enforcement of parking regulations.
(a) A vehicle parked in any location without authorization, pursuant to a fraudulent, fabricated, copied or altered parking permit, or parked contrary to the directions of posted signs or markings, shall be subject to any penalties imposed by this section and the vehicle may be removal from the Agency installation at the owner's risk and expense. The Central Intelligence Agency assumes no responsibility for the payment of any fees or costs related to the removal and/or storage of the vehicle which may be charged to the owner of the vehicle by the towing organization.

(b) The use, attempted use or possession of a fraudulent, fabricated, copied or altered parking permit is prohibited.

(c) The blocking of entrances, driveways, sidewalks, paths, loading platforms, or fire hydrants on an Agency installation is prohibited.

(d) This section may be supplemented or the applicability suspended from time to time by the Director of the Center for CIA Security, or by his or her designee, by the issuance and posting of such parking directives as may be required, and when so issued and posted, such directives shall the same force and effects as if made a part thereof.

(e) Proof that a vehicle was parked in violation of the regulations of this section or directives may be taken as prima facie evidence that the registered owner was responsible for the violation.

32 CFR Section 1903.6: Admission on to an Agency installation.

(a) Access on to any Agency installation shall be controlled and restricted to ensure the orderly and secure conduct of Agency business. Admission on to an Agency installation or into a restricted area on an Agency installation shall be limited to Agency employees and other persons with proper authorization.

(b) All persons entering on to or when on an Agency installation shall, when required and/or requested, produce and display proper identification to authorized persons.

(c) All personal property, including but not limited to any packages, briefcases, other containers or vehicles brought on to, on, or being removed from an Agency installation are subject to inspection and search by authorized persons.

(d) A full search of a person may accompany an investigative stop or an arrest.

(e) Persons entering on to an Agency installation or into a restricted area who refuse to permit an inspection and search will be denied further entry and will be ordered to leave the Agency installation or restricted area pursuant to § 1903.7(a) of this part.

(f) All persons entering on to or when on any Agency installation shall comply with all official signs of a prohibitory, regulatory, or directory nature at all times while on the Agency installation.

(g) All persons entering on to or when on any Agency installation shall comply with the instructions or directions of authorized persons.

32 CFR Section 1903.7: Trespassing.

(a) Entering, or remaining on any Agency installation without proper authorization is prohibited. Failure to obey an order to leave given under this
section by an authorized person, or reentry or attempted reentry onto the Agency installation after being ordered to leave or after being instructed not to reenter by an authorized person under this section is also prohibited.

(b) Any person who violates the provisions of this part may be ordered to leave the Agency installation by an authorized person. A violator's reentry may also be prohibited.

32 CFR Section 1903.8: Interfering with Agency functions.
The following are prohibited:

(a) Interference.

Threatening, resisting, intimidating, or intentionally interfering with a government employee or agent engaged in an official duty, or on account of the performance of an official duty.

(b) Violation of a lawful order.

Violating the lawful order of an authorized person to maintain order and control, public access and movement during fire fighting operations, law enforcement actions, and emergency operations that involve a threat to public safety or government resources, or other activities where the control of public movement and activities is necessary to maintain order and public health or safety.

(c) False information.

Knowingly giving false information:
(1) To an authorized person investigating an accident or violation of law or regulation; or
(2) On an application for a permit.

(d) False report.

Knowingly giving a false report for the purpose of misleading an authorized person in the conduct of official duties, or making a false report that causes a response by the government to a fictitious event.

32 CFR Section 1903.9: Explosives.
(a) Using, possessing, storing, or transporting explosives, blasting agents, ammunition or explosive materials is prohibited on any Agency installation, except as authorized by the Director of the Center for CIA Security. When permitted, the use, possession, storage, and transportation shall be in accordance with applicable Federal and State laws, and shall also be in accordance with applicable Central Intelligence Agency rules and/or regulations.

(b) Using, possessing, storing, or transporting items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes is prohibited.


32 CFR Section 1903.10: Weapons.
(a) Except as provided in paragraph (c) of this section, knowingly possessing or causing to be present a weapon on an Agency installation, or attempting to do so is prohibited.
(b) Knowingly possessing or causing to be present a weapon on an Agency installation, incident to hunting or other lawful purposes is prohibited.
(c) This section does not apply—
(1) Where Title 18 U.S.C. 930 applies;
(2) To any person who has received authorization from the Director of the Center for CIA Security, or from his or her designee to possess, carry, transport, or use a weapon in support of the Agency's mission or for other lawful purposes as determined by the Director of the Center for CIA Security;
(3) To the lawful performance of official duties by an officer, agent, or employee of the United States, a State, or a political subdivision thereof, who is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law; or
(4) To the possession of a weapon by a Federal official or a member of the Armed Forces if such possession is authorized by law.

32 CFR Section 1903.11: Restrictions on photographic, transmitting, and recording equipment.
(a) Except as otherwise authorized under this section, the following are prohibited on Agency installations:
(1) Possessing a camera, other visual or audio recording devices, or electronic transmitting equipment of any kind.
(2) Carrying a camera, other visual or audio recording devices, or electronic transmitting equipment of any kind.
(3) Using a camera, other visual or audio recording devices, or electronic transmitting equipment of any kind.
(b) This section does not apply to any person using, possessing or storing a government or privately owned cellular telephone or pager while on any Agency installation. The Central Intelligence Agency may regulate or otherwise administratively control cellular telephones and pagers outside the provisions of this part.
(c) This section does not apply to any officer, agent, or employee of the United States, a State, or a political subdivision thereof, who may enter on to an Agency installation to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law.
(d) This section does not apply to any person who has received approval from the Director of the Center for CIA Security, or from his or her designee to carry, transport, or use a camera, other visual or audio recording devices, or electronic transmitting equipment while on an Agency installation.

32 CFR Section 1903.12: Alcoholic beverages and controlled substance.

Page 1055
(a) Alcoholic beverages.

The possession, transportation of alcoholic beverages in closed containers and their consumption on an Agency installation will be administratively controlled by the Agency outside the provisions of this part.

(b) Controlled substances.

The following are prohibited on an Agency installation:
(1) The delivery of a controlled substance, except when distribution is made by a licensed physician or pharmacist in accordance with applicable Federal or State law, or as otherwise permitted by Federal or State law. For the purpose of this paragraph, delivery means the actual, attempt, or constructive transfer of a controlled substance.
(2) The possession of a controlled substance, unless such substance was obtained by the possessor directly from, or pursuant to a valid prescription or ordered by, a licensed physician or pharmacist, or as otherwise allowed by Federal or State law.

32 CFR Section 1903.13: Intoxicated on an Agency installation.
Presence on an Agency installation when under the influence of alcohol, a drug, or a controlled substance or a combination thereof to a degree that interferes with, impedes or hinders the performance of the official duties of any government employee, or damages government or personal property is prohibited.

32 CFR Section 1903.14: Disorderly conduct.
A person commits disorderly conduct when, with intent to cause public alarm, nuisance, jeopardy, or violence, or knowingly or recklessly creating a risk thereof, such person commits any of the following prohibited acts:
(a) Engages in fighting or threatening, or in violent behavior.
(b) Acts in a manner that is physically threatening or menacing, or acts in a manner that is likely to inflict injury or incite an immediate breach of peace.
(c) Makes noises that are unreasonable considering the nature and purpose of the actor’s conduct, location, time of day or night, and other factors that would govern the conduct of a reasonable prudent person under the circumstances.
(d) Uses obscene language, an utterance, or gesture, or engages in a display or act that is obscene.
(e) Impedes or threatens the security of persons or property, or disrupts the performance of official duties by employees, officers, contractors or visitors on an Agency installation or obstructs the use of areas on an Agency installation such as entrances, foyers, lobbies, corridors, concourses, offices, elevators, stairways, roadways, driveways, walkways, or parking lots.

32 CFR Section 1903.15: Preservation of property.
The following are prohibited:

(a) Property Damage.
Destroying or damaging private property.

(b) Theft.

The theft of private property, except where Title 18 U.S.C. 661 applies.

(c) Creation of hazard.

The creation of hazard to persons or things, the throwing of articles of any kind from or at buildings, vehicles, or persons while on an Agency installation.

(d) Improper disposal.

The improper disposal of trash or rubbish while on an Agency installation.

32 CFR Section 1903.16: Restriction on animals.
Animals, except for those animals used for the assistance of persons with disabilities, or animals under the charge and control of the Central Intelligence Agency, shall not be brought onto an Agency installation for other than official purposes.

32 CFR Section 1903.17: Soliciting, vending, and debt collection.
Commercial or political soliciting, vending of all kinds, displaying or distributing commercial advertising, collecting private debts or soliciting alms on any Agency installation is prohibited. This does not apply to:
(a) National or local drives for funds for welfare, health, or other purposes as authorized by Title 5 CFR parts 110 and 950 as amended and sponsored or approved by the Director of Central Intelligence, or by his or her designee.
(b) Personal notices posted on authorized bulletin boards and in compliance with Central Intelligence Agency rules governing the use of such authorized bulletin boards advertising to sell or rent property of Central Intelligence Agency employees or their immediate families.

32 CFR Section 1903.18: Distribution of materials.
Distributing, posting, or affixing materials, such as pamphlets, handbills, or flyers, on any Agency installation is prohibited except as authorized by § 1903.17(b), or by other authorization from the Director of the Center for CIA Security, or from his or her designee.

32 CFR Section 1903.19: Gambling.
Gambling in any form, or the operation of gambling devices, is prohibited. This prohibition shall not apply to the vending or exchange of chances by licensed blind operators of vending facilities for any lottery set forth in a State law and authorized by the provisions of the Randolph-Sheppard Act (Title 20 U.S.C. 107 et seq.).
32 CFR Section 1903.20: Penalties and effects on other laws.

(a) Whoever shall be found guilty of violating any rule or regulation enumerated in this part is subject to the penalties imposed by Federal law for the commission of a Class B misdemeanor offense.

(b) Nothing in this part shall be construed to abrogate or supersede any other Federal law or any non-conflicting State or local law, ordinance or regulation applicable to any location where the Agency installation is situated.
32 CFR PART 1904—PROCEDURES GOVERNING ACCEPTANCE
OF SERVICE OF PROCESS

1904.1: Scope and purpose.
1904.2: Definitions.
1904.3: Procedures governing acceptance of service of process.
1904.4: Notification to CIA Office of General Counsel.
1904.5: Authority of General Counsel.

Authority:
50 U.S.C. 403g; 50 U.S.C. 403(d)(3); E.O. 12333 sections 1.8(h), 1.8(i), 3.2.

Source:
56 FR 41458, Aug. 21, 1991, unless otherwise noted.

32 CFR Section 1904.1: Scope and purpose.
(a) This part sets forth the limits of authority of CIA personnel to accept service of process on behalf of the CIA or any CIA employee.
(b) This part is intended to ensure the orderly execution of the Agency's affairs and not to impede any legal proceeding.
(c) CIA regulations concerning employee responses to demands for production of official information in proceedings before federal, state, or local government entities are set out in part 1905 of this chapter.

32 CFR Section 1904.2: Definitions.

(a) Agency or CIA

means the Central Intelligence Agency and include all staff elements of the Director of Central Intelligence.

(b) Process

means a summons, complaint, subpoena, or other official paper (except garnishment orders) issued in conjunction with a proceeding or hearing being conducted by a federal, state, or local governmental entity of competent jurisdiction.

(c) Employee
means any CIA officer, any staff, contract, or other employee of CIA, any person including independent contractors associated with or acting for or on behalf of CIA, and any person formerly having such a relationship with CIA.

(d) General Counsel

includes the Deputy General Counsel or Acting General Counsel.

32 CFR Section 1904.3: Procedures governing acceptance of service of process.

(a) Service of Process Upon the CIA or a CIA Employee in An Official Capacity

(1) Personal service.
Unless otherwise expressly authorized by the General Counsel, or designee, personal service of process may be accepted only by attorneys of the Office of General Counsel at CIA Headquarters in Langley, Virginia.

(2) Mail service.
Where service of process by registered or certified mail is authorized by law, unless expressly directed otherwise by the General Counsel or designee, such process may only be accepted by attorneys of the Office of General Counsel. Process by mail should be addressed as follows: Litigation Division, Office of General Counsel, Central Intelligence Agency, Washington, DC 20505.

(b) Service of Process Upon a CIA Employee Solely in An Individual Capacity

(1) General.
Consistent with section 6 of the CIA Act of 1949, as amended, 50 U.S.C. 403g, CIA will not provide the name or address of any current or former employee of CIA to individuals or entities seeking to serve process upon such employee solely in his or her individual capacity, even where the matter is related to CIA activities.

(2) Personal Service.
Subject to the sole discretion of appropriate officials of the CIA, process servers generally will not be allowed to enter CIA facilities or premises for the purpose of serving process upon any CIA employee solely in his or her individual capacity. The Office of General Counsel is not authorized to accept service of process on behalf of a CIA employee—except the Director and Deputy Director of Central Intelligence—in his or her individual capacity.

(3) Mail Service.
Unless otherwise expressly authorized by the General Counsel, or designee, CIA personnel are not authorized to accept or forward mailed service of process directed to any CIA employee in his or her individual capacity. Any such process will be returned to the sender via appropriate postal channels.
(c) Service of Process Upon a CIA Employee in A Combined Official and Individual Capacity.

Unless expressly directed otherwise by the General Counsel, or designee, any process to be served upon a CIA employee in his or her combined official and individual capacity, in person or by mail, can be accepted only by attorneys of the Office of General Counsel at CIA Headquarters in Langley, Virginia.

(d) The documents for which service is accepted in official capacity only shall be stamped “Service Accepted in Official Capacity Only.”

Acceptance of service of process shall not constitute an admission or waiver with respect to jurisdiction, propriety of service, improper venue, or any other defense in law or equity available under the laws or rules applicable to the service of process.

32 CFR Section 1904.4: Notification to CIA Office of General Counsel.
A CIA employee who receives or has reason to expect service of process in an individual, official, or combined individual and official capacity, in a matter that may involve testimony or the furnishing of documents and that could reasonably be expected to involve Agency interests, shall promptly notify the Litigation Division, Office of General Counsel (703-874-3118). Such notification should be given prior to providing the requestor, counsel or other representative any Agency information, and prior to accepting service of process.

32 CFR Section 1904.5: Authority of General Counsel.
Any questions concerning interpretation of this regulation shall be referred to the Office of General Counsel for resolution.
32 CFR PART 1905—PRODUCTION OF OFFICIAL RECORDS OR DISCLOSURE OF OFFICIAL INFORMATION IN PROCEEDINGS BEFORE FEDERAL, STATE OR LOCAL GOVERNMENTAL ENTITIES OF COMPETENT JURISDICTION

- 1905.1: Scope and purpose.
- 1905.2: Definitions.
- 1905.3: General.
- 1905.4: Procedure for production.

**Authority:**

**Source:**
56 FR 41459, Aug. 21, 1991, unless otherwise noted.

32 CFR Section 1905.1: Scope and purpose.
This part sets forth the policy and procedures with respect to the production or disclosure of (a) material contained in the files of CIA, (b) information relating to or based upon material contained in the files of CIA, and (c) information acquired by any person while such person was an employee of CIA as part of the performance of that person's official duties or because of that person's association with CIA.

32 CFR Section 1905.2: Definitions.
For the purpose of this part:

(a) CIA or Agency
means the Central Intelligence Agency and includes all staff elements of the Director of Central Intelligence.

(b) Demand
means any subpoena, order, or other legal summons (except garnishment orders) that is issued by a federal, state, or local governmental entity of competent jurisdiction with the authority to require a response on a particular matter, or a request for appearance of an individual where a demand could issue.

(c) Employee
means any officer, any staff, contract, or other employee of CIA; any person including independent contractors associated with or acting on behalf of CIA; and any person formerly having such a relationship with CIA.

(d) Production or produce

means the disclosure of:
(1) Any material contained in the files of CIA; or
(2) Any information relating to material contained in the files of CIA, including but not limited to summaries of such information or material, or opinions based on such information or material; or
(3) Any information acquired by persons while such persons were employees of CIA as a part of the performance of their official duties or because of their official status or association with CIA; in response to a demand upon an employee of CIA.

(e) General Counsel

includes the Deputy General Counsel or Acting General Counsel.

32 CFR Section 1905.3: General.
(a) No employee shall produce any materials or information in response to a demand without prior authorization as set forth in this part. This part applies to former employees to the extent consistent with applicable nondisclosure agreements.
(b) This part is intended only to provide procedures for responding to demands for production of documents or information, and is not intended to, does not, and may not be relied upon to, create any right or benefit, substantive or procedural, enforceable by any party against the United States.

32 CFR Section 1905.4: Procedure for production.
(a) Whenever a demand for production is made upon an employee, the employee shall immediately notify the Litigation Division, Office of General Counsel, Central Intelligence Agency, Washington, DC 20505 (703/874-3118), which shall follow the procedures set forth in this section.
(b) The General Counsel of CIA and Deputy Directors or Heads of Independent Offices with responsibility for the information sought in the demand, or their designees, shall determine whether any information or materials may properly be produced in response to the demand, except that the Office of General Counsel may assert any and all legal defenses and objections to the demand available to CIA prior to the start of any search for information responsive to the demand. CIA may, in its sole discretion, decline to begin any search for information responsive to the demand until a final and non-appealable disposition of any such defenses and objections raised by CIA has been made by the entity or person that issued the demand.
(c) CIA officials shall consider the following factors, among others, in reaching a decision:
(1) Whether production is appropriate in light of any relevant privilege;
(2) Whether production is appropriate under the applicable rules of discovery or the procedures governing the case or matter in which the demand arose; and
(3) Whether any of the following circumstances apply:
   (i) Disclosure would violate a statute, including but not limited to the Privacy Act of 1974, as amended, 5 U.S.C. 552a;
   (ii) Disclosure would be inconsistent with the statutory responsibility of the Director of Central Intelligence to protect intelligence sources and methods;
   (iii) Disclosure would violate a specific CIA regulation or directive;
   (iv) Disclosure would reveal classified information;
   (v) Disclosure would improperly reveal trade secrets or proprietary confidential information without the owner's consent; or
   (vi) Disclosure would unduly interfere with the orderly conduct of CIA's functions.
(d) If oral or written testimony is sought by a demand in a case or matter in which the CIA is not a party, a reasonably detailed description of the testimony sought, in the form of an affidavit or, if that is not feasible, a written statement, by the party seeking the testimony or by the party's attorney must be furnished to the CIA Office of General Counsel.
(e) The Office of General Counsel shall be responsible for notifying the appropriate employees and other persons of all decisions regarding responses to demands and providing advice and counsel as to the implementation of such decisions.
(f) If response to a demand is required before a decision is made whether to provide the documents or information sought by the demand, an attorney from the Office of General Counsel, after consultation with the Department of Justice, shall appear before and furnish the court or other competent authority with a copy of this Regulation and state that the demand has been or is being, as the case may be, referred for the prompt consideration of the appropriate CIA officials, and shall respectfully request the court or other authority to stay the demand pending receipt of the requested instructions.
(g) If the court or other authority declines to stay the demand pending receipt of instructions in response to a request made in accordance with § 1905.4(g), or rules that the demand must be complied with irrespective of instructions rendered in accordance with this part not to produce the material or disclose the information sought, the employee upon whom the demand has been made shall, if so directed by the General Counsel of CIA, or designee, respectfully decline to comply with the demand under the authority of United States ex rel. Touhy v. Ragen, 340 U.S. 462 (1951), and this Regulation.
(h) With respect to any function granted to CIA officials in this part, such officials are authorized to delegate in writing their authority in any case or matter or category thereof to subordinate officials.
(i) Any nonemployee who receives a demand for the production or disclosure of CIA information acquired because of that person's association or contacts with
CIA should notify CIA's Office of General Counsel, Litigation Division (703/874-3118) for guidance and assistance. In such cases the provisions of this regulation shall be applicable.
32 CFR PART 1906—ENFORCEMENT OF NONDISCRIMINATION ON THE BASIS OF HANDICAP IN PROGRAMS OR ACTIVITIES CONDUCTED BY THE CENTRAL INTELLIGENCE AGENCY

1906.101: Purpose.
1906.102: Application.
1906.103: Definitions.
1906.104-1906.109: [Reserved]
1906.110: Self-evaluation.
1906.111: Notice.
1906.112-1906.129: [Reserved]
1906.130: General prohibitions against discrimination.
1906.131-1906.139: [Reserved]
1906.140: Employment.
1906.141-1906.148: [Reserved]
1906.149: Program accessibility: Discrimination prohibited.
1906.150: Program accessibility: Existing facilities.
1906.152-1906.159: [Reserved]
1906.160: Communications.
1906.161-1906.169: [Reserved]
1906.170: Compliance procedures.

Authority:

Source:
57 FR 39610, Sept. 1, 1992, unless otherwise noted.
32 CFR Section 1906.101: Purpose.
The purpose of this part is to effectuate section 119 of the Rehabilitation, Comprehensive Services, and Developmental Disabilities Amendments of 1978, which amended section 504 of the Rehabilitation Act of 1973 to prohibit discrimination on the basis of handicap in programs or activities conducted by Executive agencies or the United States Postal Service.

32 CFR Section 1906.102: Application.
This part applies to all programs or activities conducted by the Agency except for programs or activities conducted outside the United States that do not involve handicapped persons in the United States. This regulation will apply to the Agency only to the extent consistent with the National Security Act of 1947 (50 U.S.C. 402 et seq.), as amended; the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.), as amended; and other applicable law.

32 CFR Section 1906.103: Definitions.
For purposes of this part, the following terms means—

Assistant Attorney General
means the Assistant Attorney General, Civil Rights Division, United States Department of Justice.

Auxiliary aids
means services or devices that enable persons with impaired sensory, manual, or speaking skills to have an equal opportunity to participate in, and enjoy the benefits of, programs or activities conducted by the Agency. For example, auxiliary aids useful for persons with impaired vision include readers, materials in braille, audio recordings, and other similar services and devices. Auxiliary aids useful for persons with impaired hearing include telephone handset amplifiers, telephones compatible with hearing aids, telecommunication devices for deaf persons (TDD's), interpreters, notetakers, written materials, and other similar services and devices. The Central Intelligence Agency may prohibit from any of its facilities any auxiliary aid, or category of auxiliary aid, that the Office of Security (OS) determines creates a security risk or potential security risk. OS reserves the right to examine any auxiliary aid brought into an Agency facility.

Complete complaint
means a written statement that contains the complainant's name and address and describes the Agency's alleged discriminatory action in sufficient detail to inform the Agency of the nature and date of the alleged violation of section 504. It must be signed by the complainant or by someone authorized to do so on his or
her behalf. Complaints filed on behalf of classes or third parties must describe or identify (by name, if possible) the alleged victims of discrimination.

Director

means the Director of Central Intelligence or an official or employee of the Agency acting for the Director under a delegation of authority.

Facility

means all or any portion of buildings, structures, equipment, roads, walks, parking lots, rolling stock or other conveyances or other real or personal property.

Individual with handicaps

means any person who has a physical or mental impairment that substantially limits one or more major life activities, has a record of such an impairment, or is regarded as having such an impairment. As used in this definition, the phrase—

(1) Physical or mental impairment
includes—
(i) Any physiological disorder or condition, cosmetic disfigurement, or anatomical loss affecting one or more of the following body systems: Cardiovascular; Neurological; musculoskeletal; special sense organs; respiratory, including speech organs; reproductive; digestive; genitourinary; hemic and lymphatic; skin; and endocrine; or
(ii) Any mental or psychological disorder, such as mental retardation, organic brain syndrome, emotional or mental illness, and specific learning disabilities. The term “physical or mental impairment” includes, but is not limited to, such diseases and conditions as orthopedic, visual, speech, and hearing impairments, cerebral palsy, epilepsy, muscular dystrophy, multiple sclerosis, cancer, heart disease, diabetes, mental retardation, emotional illness, drug addiction, and alcoholism.

(2) Major life activities
includes functions such as caring for one's self, performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, and working;

(3) Has a record of such an impairment
means has a history of, or has been misclassified as having a mental or physical impairment that substantially limits one or more major life activities.

(4) Is regarded as having an impairment
means—
(i) Has a physical or mental impairment that does not substantially limit major life activities but is treated by the Agency as constituting such a limitation;
(ii) Has a physical or mental impairment that substantially limits major life activities only as a result of the attitudes of others toward the impairment; or
(iii) Has none of the impairments defined in paragraph (1) of this definition but is treated by the Agency as having such an impairment.

Qualified individual with handicaps

means—
(1) With respect to any Agency program or activity under which a person is required to perform services or to achieve a level of accomplishment, an individual with handicaps who meets the essential eligibility requirements and who can achieve the purpose of the program or activity without modifications in the program or activity that the Agency can demonstrate would result in a fundamental alteration in its nature;
(2) With respect to any other Agency program or activity, an individual with handicaps who meets the essential eligibility requirements for participation in, or receipt of benefits from, that program or activity; and
(3) Qualified handicapped person as that term is defined for purposes of employment in 29 CFR 1613.702(f), which is made applicable to this part by § 1906.140.

Section 504


32 CFR Section 1906.104 - 1906.109: [Reserved]

32 CFR Section 1906.110: Self-evaluation.
(a) The Agency shall, within one year of the effective date of this part, evaluate its current policies and practices, and the effect thereof, that do not or may not meet the requirements of this part, and to the extent modification of any of those policies and practices is required, the Agency shall proceed to make the necessary modifications.
(b) The Agency shall provide an opportunity to interested persons, including individuals with handicaps or organizations representing individuals with
handicaps to participate in the self-evaluation process by submitting comments (both oral and written).
(c) The Agency shall, for at least 3 years following completion of the self-evaluation, maintain on file, and make available for public inspection—
(1) A description of areas examined and any problems identified; and
(2) A description of any modifications made.

32 CFR Section 1906.111: Notice.
The Agency shall make available, to employees, applicants, participants, beneficiaries, and other interested persons, such information regarding the provisions of this part and its applicability to the programs or activities conducted by the Agency, and make that information available to them in such manner as the Director finds necessary to apprise those persons of the protections against discrimination assured them by section 504 and the regulations in this part.

32 CFR Section 1906.112 - 1906.129: [Reserved]

32 CFR Section 1906.130: General prohibitions against discrimination.
(a) No qualified individual with handicaps shall, on the basis of handicap, be excluded from participation in, be denied the benefits of, or otherwise be subjected to discrimination under, any program or activity conducted by the Agency.
(b)(1) The Agency, in providing any aid, benefit, or service, may not, directly or through contractual, licensing, or other arrangements, on the basis of handicap:
   (i) Deny a qualified individual with handicap the opportunity to participate in or benefit from the aid, benefit, or service;
   (ii) Deny a qualified individual with handicaps an opportunity to obtain the same result, to gain the same benefit, to reach the same level of achievement as that provided to others;
   (iii) Provide a qualified individual with handicaps with an aid, benefit, or service that is not as effective in affording equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement as that provided to others;
   (iv) Provide different or separate aid, benefits, or services to individuals with handicaps or to any class of individuals with handicaps than is provided to others unless that action is necessary to provide qualified individuals with handicaps with aid, benefits, or services that are as effective as those provided to others;
   (v) Deny a qualified individual with handicaps the opportunity to participate as a member of planning or advisory boards; or
   (vi) Otherwise limit a qualified individual with handicaps in the enjoyment of any right, privilege, advantage, or opportunity enjoyed by others receiving the aid, benefit, or service.
(2) The Agency may not deny a qualified individual with handicaps the opportunity to participate in programs or activities that are not separate or different, despite the existence of permissibly separate or different programs or activities.
(3) The Agency may not, directly or through contractual or other arrangements, utilize criteria or methods of administration the purpose or effect of which would—
(i) Subject qualified individuals with handicaps to discrimination on the basis of handicap; or
(ii) Defeat or substantially impair accomplishment of the objectives of a program or activity with respect to individuals with handicaps.
(4) The Agency may not, in determining the site or location of a facility, make selections the purpose or effect of which would—
(i) Exclude individuals with handicaps from, deny them the benefits of, or otherwise subject them to discrimination under, any program or activity conducted by the Agency; or
(ii) Defeat or substantially impair the accomplishment of the objectives of a program or activity with respect to individuals with handicaps.
(5) The Agency, in the selection of procurement contractors, may not use criteria that subject qualified individuals with handicaps to discrimination on the basis of handicap.
(6) The Agency may not administer a licensing or certification program in a manner that subjects qualified individuals with handicaps to discrimination on the basis of handicap, nor may the Agency establish requirements for the programs or activities of licensees or certified entities that subject qualified individuals with handicaps to discrimination on the basis of handicap. However, the programs or activities of entities that are licensed or certified by the Agency are not, themselves, covered by this part.
(c) The exclusion of nonhandicapped persons from the benefits or a program limited by Federal statute or Executive Order to individuals with handicaps or the exclusion of a specific class of individuals with handicaps from a program limited by Federal statute or Executive Order to a different class of individuals with handicaps is not prohibited by this part.
(d) The Agency shall administer programs and activities in the most integrated setting appropriate to the needs of qualified individuals with handicaps.

32 CFR Section 1906.131 - 1906.139: [Reserved]

32 CFR Section 1906.140: Employment.
No qualified individual with handicaps shall, solely on the basis of handicap, be subjected to discrimination in employment under any program or activity conducted by the Agency. The definitions, requirements, and procedures of section 501 of the Rehabilitation Act of 1979 (29 U.S.C. 791), as established by the Equal Employment Opportunity Commission in 29 CFR part 1613, shall apply to employment in federally conducted programs or activities.
32 CFR Section 1906.141 - 1906.148: [Reserved]

32 CFR Section 1906.149: Program accessibility: Discrimination prohibited. Excep
t as otherwise provided in § 1906.150, no qualified individual with handicaps shall, because the Agency's facilities are inaccessible to or unusable by individuals with handicaps, be denied the benefits of, be excluded from participation in, or otherwise be subjected to discrimination under any program or activity conducted by the Agency.

32 CFR Section 1906.150: Program accessibility: Existing facilities.

(a) General.

The Agency shall operate each program or activity so that the program or activity, viewed in its entirety, is readily accessible to and usable by individuals with handicaps. This program does not—
(1) Necessarily require the Agency to make each of its existing facilities accessible to and usable by individuals with handicaps;
(2)(i) Require the Agency to take any action that it can demonstrate would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens.
(ii) The Agency has the burden of proving that compliance with § 1906.150(a) would result in that alteration or those burdens.
(iii) The decision that compliance would result in that alteration or those burdens must be made by the Director after considering all of the Agency's resources available for use in the funding and operation of the conducted program or activity, and must be accompanied by a written statement of the reasons for reaching that conclusion.
(iv) If an action would result in that alteration or those burdens, the Agency shall take any other action that would not result in the alteration or burdens but would nevertheless ensure that individuals with handicaps receive the benefits and services of the program or activity.

(b) Methods.

(1) The Agency may comply with the requirements of this section through such means as redesign of equipment, reassignment of services to accessible buildings, assignment of aides to beneficiaries, home visits, delivery of services at alternate accessible sites, alteration of existing facilities and construction of new facilities, use of accessible rolling stock, or any other methods that result in making its programs or activities readily accessible to and usable by individuals with handicaps.
(2) The Agency is not required to make structural changes in existing facilities if other methods are effective in achieving compliance with this section.
(3) The Agency, in making alterations to existing buildings, shall meet accessibility requirements to the extent compelled by the Architectural Barriers Act of 1968, as amended (42 U.S.C. 4151-4157), and any regulations implementing that Act.

(4) In choosing among available methods for meeting the requirements of this section, the Agency shall give priority to those methods that offer programs and activities to qualified individuals with handicaps in the most integrated setting appropriate.

(c) Time period for compliance.

The Agency shall comply with the obligations established under this section within 60 days of the effective date of this part except that if structural changes in facilities are undertaken, the changes shall be made within 3 years of the effective date of this part, but in any event as expeditiously as possible.

(d) Transition plan.

(1) In the event that structural changes to facilities will be undertaken to achieve program accessibility, the Agency shall develop, within 6 months of the effective date of this part, a transition plan setting forth the steps necessary to complete those changes.

(2) The Agency shall provide an opportunity to interested persons, including individuals with handicaps or organizations representing individuals with handicaps, to participate in the development of the transition plan by submitting comments (both oral and written). A copy of the transition plan must be made available for public inspection.

(3) The plan must, at a minimum—
   (i) Identify physical obstacles in the Agency's facilities that limit the accessibility of its programs or activities to individuals with handicaps;
   (ii) Describe in detail the methods that will be used to make the facilities accessible;
   (iii) Specify the schedule for taking the steps necessary to achieve compliance with this section and, if the time period of the transition plan is longer than one year, identify steps that will be taken during each year of the transition period; and
   (iv) Indicate the official responsible for implementation of the plan.


Each building or part of a building that is constructed or altered by, on behalf of, or for the use of, the Agency shall be designed, constructed, or altered so as to be readily accessible to and usable by individuals with handicaps. The definitions, requirements, and standards of the Architectural Barriers Act of 1968 (42 U.S.C. 4151-4175), as established in 41 CFR 101-19.600 to 101-19.607, apply to buildings covered by this section.
32 CFR Section 1906.152 - 1906.159: [Reserved]

32 CFR Section 1906.160: Communications.
(a) The Agency shall take appropriate steps to ensure effective communication with applicants, participants, personnel of other Federal entities, and members of the public as follows:
(1)(i) The Agency shall furnish appropriate auxiliary aids if necessary to afford an individual with handicaps an equal opportunity to participate in, and enjoy the benefits of, a program or activity conducted by the Agency.
(ii) In determining what type of auxiliary aid is necessary, the Agency shall give primary consideration to the requests of the individual with handicaps.
(2) Where the Agency communicates with applicants and beneficiaries by telephone, telecommunication devices for deaf persons (TDD's) or equally effective telecommunication systems shall be used to communicate with persons with impaired hearing.
(b) The Agency shall ensure that interested persons, including persons with impaired vision or hearing, can obtain information as to the existence and location of accessible services, activities, and facilities.
(c) The Agency shall provide signage at a primary entrance to each of its inaccessible facilities, directing users to a location at which they can obtain information about accessible facilities. The international symbol for accessibility shall be used at each primary entrance of an accessible facility.
(d) This section does not require the Agency to take any action that it can demonstrate would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens. In those circumstances where Agency personnel believe that the proposed action would fundamentally alter the program or activity or would result in undue financial and administrative burdens, the Agency has the burden of proving that compliance with § 1906.160 would result in such alteration or burdens. The decision that compliance would result in such alteration or burdens must be made by the Agency head or his or her designee after considering all Agency resources available for use in the funding and operation of the conducted program or activity and must be accompanied by a written statement of the reasons for reaching that conclusion. If an action required to comply with this section would result in such an alteration or such burdens, the Agency shall take any other action that would not result in such an alteration or such burdens but would nevertheless ensure that, to the maximum extent possible, individuals with handicaps receive the benefits and services of the program or activity.

32 CFR Section 1906.161 - 1906.169: [Reserved]

32 CFR Section 1906.170: Compliance procedures.
(a) Except as provided in paragraph (b) of this section, this section applies to all allegations of discrimination on the basis of handicap in programs and activities conducted by the Agency.
(b) The Agency shall process complaints alleging violations of section 504 with respect to employment according to the procedures established by the Equal Employment Opportunity Commission in 29 CFR part 1613 pursuant to section 501 of the Rehabilitation Act of 1973 (29 U.S.C. 791).

c) The Director, Office of Equal Employment Opportunity, is responsible for coordinating implementation of this section. Complaints may be sent to Central Intelligence Agency, Director, Office of Equal Employment Opportunity, Washington, DC 20505.

d) The Agency shall accept and investigate all complete complaints for which it has jurisdiction. All complete complaints must be filed within 180 days of the alleged act of discrimination. The Agency may extend this time period for good cause.

e) If the Agency receives a complaint over which it does not have jurisdiction, it shall promptly notify the complainant and shall make reasonable efforts to refer the complaint to the appropriate government entity.

(f) The Agency shall notify the Architectural and Transportation Barriers Compliance Board upon receipt of any complaint alleging that a building or facility that is subject to the Architectural Barriers Act of 1968, as amended (42 U.S.C. 4151-4157) is not readily accessible to and usable by individuals with handicaps.

(g) Within 180 days of the receipt of a complete complaint for which it has jurisdiction, The Agency shall notify the complainant of the results of the investigation in a letter containing—

1. Findings of fact and conclusions of law;
2. A description of a remedy for each violation found; and
3. A notice of the right to appeal.

(h) Appeals of the findings of fact and conclusions of law or remedies must be filed by the complainant within 90 days of receipt from the Agency of the letter required by § 1906.170(g). The Agency may extend this time for good cause.

(i) Timely appeals shall be accepted and processed by the Director.

(j) The Agency shall notify the complainant of the results of the appeal within 60 days of the receipt of the request. If the Agency determines that it needs additional information from the complainant, it shall have 60 days from the date it receives the additional information to make its determination on the appeal.

(k) The time limits cited in paragraphs (g) and (j) of this section may be extended with the permission of the Assistant Attorney General.

(l) The Director may delegate the authority for conducting complaint investigations to other Federal agencies, except that the authority for making the final determination may not be delegated.
32 CFR PART 1907—CHALLENGES TO CLASSIFICATION OF DOCUMENTS BY AUTHORIZED HOLDERS PURSUANT TO § 1.9 OF EXECUTIVE ORDER 12958

➤ General
  o 1907.01: Authority and purpose.
  o 1907.02: Definitions.
  o 1907.03: Contact for general information and requests.
  o 1907.04: Suggestions and complaints.

➤ Filing of Challenges
  o 1907.11: Prerequisites.
  o 1907.12: Requirements as to form.
  o 1907.13: Identification of material at issue.
  o 1907.14: Transmission.

➤ Action on Challenges
  o 1907.21: Receipt, recording, and tasking.
  o 1907.22: Challenges barred by res judicata.
  o 1907.23: Response by originator(s) and/or any interested party.
  o 1907.24: Designation of authority to hear challenges.
  o 1907.25: Action on challenge.
  o 1907.26: Notification of decision and prohibition on adverse action.

➤ Right of Appeal
  o 1907.31: Right of appeal.

Authority:
Executive Order 12958, 60 FR 19825, 3 CFR 1996 Comp., P. 333-356 (or successor orders).

Source:
62 FR 32494, June 16, 1997, unless otherwise noted.
32 CFR Section 1907.01: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement § 1.9 of Executive Order (E.O.) 12958, sec. 102 of the National Security Act of 1947, and sec. 6 of the CIA Act of 1949.

(b) Purpose.

This part prescribes procedures for authorized holders of information classified under the various provisions of E.O. 12958, or predecessor Orders, to seek a review or otherwise challenge the classified status of information to further the interests of the United States Government. This part and § 1.9 of E.O. 12958 confer no rights upon members of the general public, or authorized holders acting in their personal capacity, both of whom shall continue to request reviews of classification under the mandatory declassification review provisions set forth at § 3.6 of E.O. 12958.

32 CFR Section 1907.02: Definitions.

For purposes of this part, the following terms have the meanings as indicated:

(a) Agency or CIA

means the United States Central Intelligence Agency acting through the CIA Information and Privacy Coordinator;

(b) Authorized holders

means any member of any United States executive department, military department, the Congress, or the judiciary (Article III) who holds a security clearance from or has been specifically authorized by the Central Intelligence Agency to possess and use on official business classified information, or otherwise has Constitutional authority pursuant to their office;

(c) Days

means calendar days when the Agency is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this CFR part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

(d) Challenge

means a request in the individual’s official, not personal, capacity and in furtherance of the interests of the United States;
(e) Control

means ownership or the authority of the CIA pursuant to federal statute or privilege to regulate official or public access to records;

(f) Coordinator

means the CIA Information and Privacy Coordinator acting in the capacity of Executive Secretary of the Agency Release Panel;

(g) Information

means any knowledge that can be communicated or documentary material, regardless of its physical form, that is:
(1) Owned by, produced by or for, or under the control of the United States Government, and
(2) Lawfully and actually in the possession of an authorized holder and for which ownership and control has not been relinquished by the CIA;

(h) Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of the CIA, has a subject matter or physical interest in the documents or information at issue;

(i) Originator

means the CIA officer who originated the information at issue, or successor in office, or a CIA officer who has been delegated declassification authority for the information at issue in accordance with the provisions of this Order;

(j) This Order

means Executive Order 12958 of April 17, 1995 and published at 60 FR 19825-19843 (or successor Orders).

32 CFR Section 1907.03: Contact for general information and requests.
For information on this part or to file a challenge under this part, please direct your inquiry to the Executive Secretary, Agency Release Panel, Central Intelligence Agency, Washington, DC 20505. The commercial (non-secure) telephone is (703) 613-1287; the classified (secure) telephone for voice and facsimile is (703) 613-3007.

32 CFR Section 1907.04: Suggestions and complaints.
The Agency welcomes suggestions or complaints with regard to its administration of the Executive Order. Letters of suggestion or complaint should identify the
specific purpose and the issues for consideration. The Agency will respond to all substantive communications and take such actions as determined feasible and appropriate.
Filing of Challenges

32 CFR Section 1907.11: Prerequisites.
The Central Intelligence Agency has established liaison and procedures with many agencies for declassification issues. Prior to reliance on this Part, authorized holders are required to first exhaust such established administrative procedures for the review of classified information. Further information on these procedures is available from the point of contact, see 32 CFR 1907.03.

32 CFR Section 1907.12: Requirements as to form.
The challenge shall include identification of the challenger by full name and title of position, verification of security clearance or other basis of authority, and an identification of the documents or portions of documents or information at issue. The challenge shall also, in detailed and factual terms, identify and describe the reasons why it is believed that the information is not protected by one or more of the § 1.5 provisions, that the release of the information would not cause damage to the national security, or that the information should be declassified due to the passage of time. The challenge must be properly classified; in this regard, until the challenge is decided, the authorized holder must treat the challenge, the information being challenged, and any related or explanatory information as classified at the same level as the current classification of the information in dispute.

32 CFR Section 1907.13: Identification of material at issue.
Authorized holders shall append the documents at issue and clearly mark those portions subject to the challenge. If information not in documentary form is in issue, the challenge shall state so clearly and present or otherwise refer with specificity to that information in the body of the challenge.

32 CFR Section 1907.14: Transmission.
Authorized holders must direct challenge requests to the CIA as specified in § 1907.03. The classified nature of the challenge, as well as the appended documents, require that the holder transmit same in full accordance with established security procedures. In general, registered U.S. mail is approved for SECRET, non-compartmented material; higher classifications require use of approved Top Secret facsimile machines or CIA-approved couriers. Further information is available from the CIA as well as corporate or other federal agency security departments.
Action on Challenges
32 CFR Section 1907.21: Receipt, recording, and tasking.
The Executive Secretary of the Agency Release Panel shall within ten (10) days record each challenge received under this Part, acknowledge receipt to the authorized holder, and task the originator and other interested parties. Additional taskings, as required during the review process, shall be accomplished within five (5) days of notification.

32 CFR Section 1907.22: Challenges barred by res judicata.
The Executive Secretary of the Agency Release Panel shall respond on behalf of the Panel and deny any challenge where the information in question has been the subject of a classification review within the previous two (2) years or is the subject of pending litigation in the federal courts.

32 CFR Section 1907.23: Response by originator(s) and/or any interested party.

(a) In general.
The originator of the classified information (document) is a required party to any challenge; other interested parties may become involved through the request of the Executive Secretary or the originator when it is determined that some or all of the information is also within their official cognizance.

(b) Determination.
These parties shall respond in writing to the Executive Secretary of the Agency Release Panel with a mandatory unclassified finding, to the greatest extent possible, and an optional classified addendum. This finding shall agree to a declassification or, in specific and factual terms, explain the basis for continued classification including identification of the category of information, the harm to national security which could be expected to result from disclosure, and, if older than ten (10) years, the basis for the extension of classification time under §§ 1.6 and 3.4 of this Order. These parties shall also provide a statement as to whether or not there is any other statutory, common law, or Constitutional basis for withholding as required by § 6.1(c) of this Order.

(c) Time.
The determination(s) shall be provided on a “first-in, first-out” basis with respect to all challenges pending under this section and shall be accomplished expeditiously taking into account the requirements of the authorized holder as well as the business requirements of the originator including their responsibilities under the Freedom of Information Act, the Privacy Act, or the mandatory declassification review provisions of this Order.
32 CFR Section 1907.24: Designation of authority to hear challenges.
The Deputy Director for Administration has designated the Agency Release Panel and the Historical Records Policy Board, established pursuant to 32 CFR 1900.41, as the Agency authority to hear and decide challenges under these regulations.

32 CFR Section 1907.25: Action on challenge.

(a) Action by Agency Release Panel.

The Executive Secretary shall place challenges ready for adjudication on the agenda at the next occurring meeting of the Agency Release Panel. The Executive Secretary shall provide a summation memorandum for consideration of the members; the complete package consisting of the challenge, the information at issue, and the findings of the originator and interested parties shall also be provided. The Agency Release Panel shall meet and decide challenges sitting as a committee of the whole. Decisions are by majority vote of those present at a meeting and shall be based on the written record and their deliberations; no personal appearances shall be permitted without the express permission of the Panel.

(b) Action by Historical Records Policy Board.

In any cases of divided vote by the ARP, any member of that body is authorized to refer the request to the CIA Historical Records Policy Board which acts as the senior corporate board for the Agency. The record compiled (the request, the memoranda filed by the originator and interested parties, and the previous decision(s)) as well as any memorandum of law or policy the referent desires to be considered, shall be certified by the Executive Secretary of the Agency Release Panel and shall constitute the official record of the proceedings and must be included in any subsequent filings.

32 CFR Section 1907.26: Notification of decision and prohibition on adverse action.
The Executive Secretary of the Agency Release Panel shall communicate the decision of the Agency to the authorized holder, the originator, and other interested parties within ten (10) days of the decision by the Panel or Board. That correspondence shall include a notice that no adverse action or retribution can be taken in regard to the challenge and that an appeal of the decision may be made to the Interagency Security Classification Appeals Panel (ISCAP) established pursuant to § 5.4 of this Order.
Right of Appeal
32 CFR Section 1907.31: Right of appeal.
A right of appeal is available to the ISCAP established pursuant to § 5.4 of this Order. Action by that body will be the subject of rules to be promulgated by the Information Security Oversight Office (ISOO).
32 CFR PART 1908—PUBLIC REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW OF CLASSIFIED INFORMATION PURSUANT TO § 3.6 OF EXECUTIVE ORDER 12958

➤ General
  o 1908.01: Authority and purpose.
  o 1908.02: Definitions.
  o 1908.03: Contact for general information and requests.
  o 1908.04: Suggestions and complaints.
➤ Filing of Mandatory Declassification Review (MDR) Requests
  o 1908.11: Preliminary information.
  o 1908.12: Requirements as to form.
  o 1908.13: Fees.
➤ Agency Action on MDR Requests
  o 1908.21: Receipt, recording, and tasking.
  o 1908.22: Requests barred by res judicata.
  o 1908.23: Determination by originator or interested party.
  o 1908.24: Notification of decision and right of appeal.
➤ Agency Action on MDR Appeals
  o 1908.31: Requirements as to time and form.
  o 1908.32: Receipt, recording, and tasking.
  o 1908.33: Determination by Deputy Director(s).
  o 1908.34: Establishment of appeals structure.
  o 1908.35: Action by appeals authority.
  o 1908.36: Notification of decision and right of further appeal.
➤ Further Appeals
  o 1908.41: Right of further appeal.

Authority:
Executive Orders 12958, 60 FR 19825, 3 CFR 1996 Comp., p. 333-356 (or successor Orders).

Source:
62 FR 32495, June 16, 1997, unless otherwise noted.

General
32 CFR Section 1908.01: Authority and purpose.

(a) Authority.
This part is issued under the authority of and in order to implement § 3.6 of Executive Order (E.O.) 12958 (or successor Orders); the CIA Information Act of 1984 (50 U.S.C. 431); sec. 102 of the National Security Act of 1947, as amended (50 U.S.C. 403); and sec. 6 of the CIA Act of 1949, as amended (5 U.S.C. 403g).

(b) Purpose.

This part prescribes procedures, subject to limitations set forth below, for members of the public to request a declassification review of information classified under the various provisions of this or predecessor Orders. Section 3.6 of E.O. 12958 and these regulations do not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, officers, or employees.

32 CFR Section 1908.02: Definitions.
For purposes of this part, the following terms have the meanings as indicated:

(a) Agency or CIA
means the United States Central Intelligence Agency acting through the CIA Information and Privacy Coordinator;

(b) Days
means calendar days when the Agency is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

(c) Control
means ownership or the authority of the CIA pursuant to Federal statute or privilege to regulate official or public access to records;

(d) Coordinator
means the CIA Information and Privacy Coordinator who serves as the Agency manager of the information review and release program instituted under the mandatory declassification review provisions of Executive Order 12958;

(e) Federal agency
means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

(f) Information
means any knowledge that can be communicated or documentary material, regardless of its physical form that is owned by, produced by or for, or under the control of the United States Government; it does not include:

(1) Information within the scope of the CIA Information Act, or
(2) Information originated by the incumbent President, White House Staff, appointed committees, commissions or boards, or any entities within the Executive Office that solely advise and assist the incumbent President;

(g) Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of the CIA, has a subject matter or physical interest in the documents or information at issue;

(h) NARA

means the National Archives and Records Administration;

(i) Originator

means the CIA officer who originated the information at issue, or successor in office, or a CIA officer who has been delegated declassification authority for the information at issue in accordance with the provisions of this Order;

(j) Presidential libraries

means the libraries or collection authorities established by statute to house the papers of former Presidents Hoover, Roosevelt, Truman, Eisenhower, Kennedy, Nixon, Ford, Carter, Reagan, Bush and similar institutions or authorities as may be established in the future;

(k) Referral

means coordination with or transfer of action to an interested party;

(l) This Order

means Executive Order 12958 of April 17, 1995 and published at 60 FR 19825-19843 (or successor Orders);

32 CFR Section 1908.03: Contact for general information and requests.
For general information on this part or to request a declassification review, please direct your communication to the Information and Privacy Coordinator, Central Intelligence Agency, Washington, DC 20505. Such inquiries will also be accepted by facsimile at (703) 613-3007. For general or status information only, the telephone number is (703) 613-1287. Collect calls cannot be accepted.
32 CFR Section 1908.04: Suggestions and complaints.
The Agency welcomes suggestions or complaints with regard to its administration of the mandatory declassification review program established under Executive Order 12958. Many requesters will receive pre-paid, customer satisfaction survey cards. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. The Agency will respond to all substantive communications and take such actions as determined feasible and appropriate.

32 CFR Section 1908.11: Preliminary information.
Members of the public shall address all communications to the point of contact specified above and clearly delineate the communication as a request under this regulation. Requests and appeals on requests received from members of the public who owe outstanding fees for information services under this Order or the Freedom of Information Act at this or another federal agency will not be accepted until such debts are resolved.

32 CFR Section 1908.12: Requirements as to form.
The request shall identify the document(s) or material(s) with sufficient specificity (e.g., National Archives and Records Administration (NARA) Document Accession Number or other applicable, unique document identifying number) to enable the Agency to locate it with reasonable effort. Broad or topical requests for records on a particular subject may not be accepted under this provision. A request for documents contained in the various Presidential libraries shall be effected through the staff of such institutions who shall forward the document(s) in question for Agency review. The requester shall also provide sufficient personal identifying information when required by the Agency to satisfy requirements of this part.

32 CFR Section 1908.13: Fees.
Requests submitted via NARA or the various Presidential libraries shall be responsible for reproduction costs required by statute or regulation. Requests made directly to this Agency will be liable for costs in the same amount and under the same conditions as specified in 32 CFR part 1900.
Agency Action on MDR Requests

32 CFR Section 1908.21: Receipt, recording, and tasking.
The Information and Privacy Coordinator shall within ten (10) days record each mandatory declassification review request received under this part, acknowledge receipt to the requester in writing (if received directly from a requester), and shall thereafter task the originator and other interested parties. Additional taskings, as required during the review process, shall be accomplished within ten (10) days of notification.

32 CFR Section 1908.22: Requests barred by res judicata.
The Coordinator shall respond to the requester and deny any request where the information in question has been the subject of a classification review within the previous two (2) years or is the subject of pending litigation in the federal courts.

32 CFR Section 1908.23: Determination by originator or interested party.
(a) In general.
The originator of the classified information (document) is a required party to any mandatory declassification review request; other interested parties may become involved through a referral by the Coordinator when it is determined that some or all of the information is also within their official cognizance.

(b) Required determinations.
These parties shall respond in writing to the Coordinator with a finding as to the classified status of the information including the category of protected information as set forth in § 1.5 of this Order, and, if older than ten (10) years, the basis for the extension of classification time under §§ 1.6 and 3.4 of this Order. These parties shall also provide a statement as to whether or not there is any other statutory, common law, or Constitutional basis for withholding as required by § 6.1(c) of this Order.

(c) Time.
This response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the originator or interested parties and consistent with the information rights of members of the general public under the Freedom of Information Act and the Privacy Act.

32 CFR Section 1908.24: Notification of decision and right of appeal.
The Coordinator shall communicate the decision of the Agency to the requester within ten (10) days of completion of all review action. That correspondence shall include a notice of a right of administrative appeal to the Agency Release Panel pursuant to § 3.6(d) of this Order.
Agency Action on MDR Appeals

32 CFR Section 1908.31: Requirements as to time and form.
Appeals of decisions must be received by the Coordinator within forty-five (45) days of the date of mailing of the Agency's initial decision. It shall identify with specificity the documents or information to be considered on appeal and it may, but need not, provide a factual or legal basis for the appeal.

32 CFR Section 1908.32: Receipt, recording, and tasking.
The Coordinator shall promptly record each appeal received under this part, acknowledge receipt to the requester, and task the originator and other interested parties. Additional taskings, as required during the review process, shall be accomplished within ten (10) days of notification.

32 CFR Section 1908.33: Determination by Deputy Director(s).
Each Deputy Director in charge of a directorate which originated or has an interest in any of the records subject to the appeal, or designee, is a required party to any appeal; other interested parties may become involved through the request of the Coordinator when it is determined that some or all of the information is also within their official cognizance. These parties shall respond in writing to the Coordinator with a finding as to the classified status of the information including the category of protected information as set forth in § 1.5 of this Order, and, if older than ten (10) years, the basis for continued classification under §§ 1.6 and 3.4 of this Order. These parties shall also provide a statement as to whether or not there is any other statutory, common law, or Constitutional basis for withholding as required by § 6.1(c) of this Order. This response shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the parties and consistent with the information rights of members of the general public under the Freedom of Information Act and the Privacy Act.

32 CFR Section 1908.34: Establishment of appeals structure.

(a) In general.

Two administrative entities have been established by the Director of Central Intelligence to facilitate the processing of administrative appeals under the mandatory declassification review provisions of this Order. Their membership, authority, and rules of procedure are as follows.

(b) Historical Records Policy Board (“HRPB” or “Board”).

This Board, the successor to the CIA Information Review Committee, acts as the senior corporate board in the CIA on all matters of information review and release. It is composed of the Executive Director, who serves as its Chair, the
Deputy Director for Administration, the Deputy Director for Intelligence, the Deputy Director for Operations, the Deputy Director for Science and Technology, the General Counsel, the Director of Congressional Affairs, the Director of the Public Affairs Staff, the Director, Center for the Study of Intelligence, and the Associate Deputy Director for Administration/Information Services, or their designees. The Board, by majority vote, may delegate to one or more of its members the authority to act on any appeal or other matter or authorize the Chair to delegate such authority, as long as such delegation is not to the same individual or body who made the initial denial. The Executive Secretary of the HRPB is the Director, Information Management. The Chair may request interested parties to participate when special equities or expertise are involved.

(c) Agency Release Panel (“ARP” or “Panel”).

The HRPB, pursuant to its delegation of authority, has established a subordinate Agency Release Panel. This Panel is composed of the Director, Information Management, who serves as its Chair; the Information Review Officers from the Directorates of Administration, Intelligence, Operations, Science and Technology, and the Director of Central Intelligence Area; the CIA Information and Privacy Coordinator; the Chief, Historical Review Group; the Chair, Publications Review Board; the Chief, Records Declassification Program; and representatives from the Offices of General Counsel and Congressional Affairs, and the Public Affairs Staff. The Information and Privacy Coordinator also serves as the Executive Secretary of the Panel. The Panel advises and assists the HRPB on all information release issues, monitors the adequacy and timeliness of Agency releases, sets component search and review priorities, reviews adequacy of resources available to and planning for all Agency release programs, and performs such other functions as deemed necessary by the Board. The Chair may request interested parties to participate when special equities or expertise are involved. The Panel, functioning as a committee of the whole or through individual members, will make final Agency decisions from appeals of initial denial decisions under E.O. 12958. Issues not resolved by the Panel will be referred by the Panel to the HRPB. Matters decided by the Panel or Board will be deemed a final decision by the Agency.

32 CFR Section 1908.35: Action by appeals authority.

(a) Action by Agency Release Panel.

The Coordinator, in his or her capacity as Executive Secretary of the Agency Release Panel, shall place appeals of mandatory declassification review requests ready for adjudication on the agenda at the next occurring meeting of the Agency Release Panel. The Executive Secretary shall provide a summation memorandum for consideration of the members, the complete record of the request consisting of the request, the document(s) (sanitized and full text) at issue, and the findings of the originator and interested parties. The Panel shall meet and decide requests
sitting as a committee of the whole. Decisions are by majority vote of those present at a meeting and shall be based on the written record and their deliberations; no personal appearances shall be permitted without the express permission of the Panel.

(b) Action by Historical Records Policy Board.

In any cases of divided vote by the ARP, any member of that body is authorized to refer the request to the CIA Historical Records Policy Board which acts as the senior corporate board for the Agency. The record compiled (the request, the memoranda filed by the originator and interested parties, and the previous decision(s)) as well as any memorandum of law or policy the referent desires to be considered, shall be certified by the Executive Secretary of the Agency Release Panel and shall constitute the official record of the proceedings and must be included in any subsequent filings.

32 CFR Section 1908.36: Notification of decision and right of further appeal.
The Coordinator shall communicate the decision of the Panel or Board to the requester, NARA, or the particular Presidential Library within ten (10) days of such decision. That correspondence shall include a notice that an appeal of the decision may be made to the Interagency Security Classification Appeals Panel (ISCAP) established pursuant to § 5.4 of this Order.

Further Appeals
32 CFR Section 1908.41: Right of further appeal.
A right of further appeal is available to the ISCAP established pursuant to § 5.4 of this Order. Action by that Panel will be the subject of rules to be promulgated by the Information Security Oversight Office (ISOO).
32 CFR PART 1909—ACCESS BY HISTORICAL RESEARCHERS AND FORMER PRESIDENTIAL APPOINTEES PURSUANT TO § 4.5 OF EXECUTIVE ORDER 12958

➢ General
  o 1909.01: Authority and purpose.
  o 1909.02: Definitions.
  o 1909.03: Contact for general information and requests.
  o 1909.04: Suggestions and complaints.
➢ Requests for Historical Access
  o 1909.11: Requirements as to who may apply.
  o 1909.12: Designations of authority to hear requests.
  o 1909.13: Receipt, recording, and tasking.
  o 1909.14: Determinations by tasked officials.
  o 1909.15: Action by hearing authority.
  o 1909.16: Action by appeal authority.
  o 1909.17: Notification of decision.
  o 1909.18: Termination of access.

Authority:
Executive Order 12958, 60 FR 19825. 3 CFR 1996 Comp., p. 333-356 (or successor Orders).

Source:
62 FR 32498, June 16, 1997, unless otherwise noted.
General

32 CFR Section 1909.01: Authority and purpose.

(a) Authority.

This part is issued under the authority of and in order to implement § 4.5 of Executive Order 12958 (or successor Orders); the CIA Information Act of 1984 (50 U.S.C. 431); sec. 102 of the National Security Act of 1947, as amended (50 U.S.C. 403); and sec. 6 of the Central Intelligence Agency Act of 1949, as amended (50 U.S.C. 403g).

(b) Purpose.

(1) This part prescribes procedures for:
   (i) Requesting access to CIA records for purposes of historical research, or
   (ii) Requesting access to CIA records as a former Presidential appointee.

(2) Section 4.5 of Executive Order 12958 and these regulations do not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, officers, or employees.

32 CFR Section 1909.02: Definitions.
For purposes of this part, the following terms have the meanings indicated:

(a) Agency or CIA

means the United States Central Intelligence Agency acting through the CIA Information and Privacy Coordinator;

(b) Agency Release Panel or Panel or ARP

means the CIA Agency Release Panel established pursuant to 32 CFR 1900.41;

(c) Days

means calendar days when the Agency is operating and specifically excludes Saturdays, Sundays, and legal public holidays. Three (3) days may be added to any time limit imposed on a requester by this part if responding by U.S. domestic mail; ten (10) days may be added if responding by international mail;

(d) Control

means ownership or the authority of the CIA pursuant to federal statute or privilege to regulate official or public access to records;

(e) Coordinator
means the CIA Information and Privacy Coordinator who serves as the Agency manager of the historical access program established pursuant to § 4.5 of this Order;

(f) Director, Center for the Study of Intelligence or “D/CSI”

means the Agency official responsible for the management of the CIA's various historical programs including the management of access granted under this section;

(g) Director of Personnel Security

means the Agency official responsible for making all security and access approvals and for effecting the necessary non-disclosure and/or pre-publication agreements as may be required;

(h) Federal agency

means any executive department, military department, or other establishment or entity included in the definition of agency in 5 U.S.C. 552(f);

(i) Former Presidential appointee

means any person who has previously occupied a policy-making position in the executive branch of the United States Government to which they were appointed by the current or former President and confirmed by the United States Senate;

(j) Historian or historical researcher

means any individual with professional training in the academic field of history (or related fields such as journalism) engaged in a research project leading to publication (or any similar activity such as academic course development) reasonably intended to increase the understanding of the American public into the operations and activities of the United States government;

(k) Information

means any knowledge that can be communicated or documentary material, regardless of its physical form that is owned by, produced by or for, or is under the control of the United States Government;

(l) Interested party

means any official in the executive, military, congressional, or judicial branches of government, United States or foreign, or U.S. Government contractor who, in the sole discretion of the CIA, has a subject matter or physical interest in the documents or information at issue;
(m) Originator

means the CIA officer who originated the information at issue, or successor in office, or a CIA officer who has been delegated declassification authority for the information at issue in accordance with the provisions of this Order;

(n) This Order

means Executive Order 12958 of April 17 1995 and published at 60 FR 19825-19843 (or successor Orders).

32 CFR Section 1909.03: Contact for general information and requests.
For general information on this Part, to inquire about historical access to CIA records, or to make a formal request for such access, please direct your communication in writing to the Information and Privacy Coordinator, Central Intelligence Agency, Washington, DC. 20505. Inquiries will also be accepted by facsimile at (703) 613-3007. For general information only, the telephone number is (703) 613-1287. Collect calls cannot be accepted.

32 CFR Section 1909.04: Suggestions and complaints.
The Agency welcomes suggestions or complaints with regard to its administration of the historical access program established pursuant to Executive Order 12958. Letters of suggestion or complaint should identify the specific purpose and the issues for consideration. The Agency will respond to all substantive communications and take such actions as determined feasible and appropriate.

Requests for Historical Access
32 CFR Section 1909.11: Requirements as to who may apply.

(a) Historical researchers

(1) In general.
Any historian engaged in a historical research project as defined above may submit a request in writing to the Coordinator to be given access to classified information for purposes of that research. Any such request shall indicate the nature, purpose, and scope of the research project.

(2) Additional considerations.
In light of the very limited resources for the Agency's various historical programs, it is the policy of the Agency to consider applications for historical research privileges only in those instances where the researcher's needs cannot be satisfied through requests for access to reasonably described records under the Freedom of Information Act or the mandatory declassification review provisions of Executive Order 12958 and where issues of internal resource availability and
fairness to all members of the historical research community militate in favor of a particular grant.

(b) Former Presidential appointees.

Any former Presidential appointee as defined herein may also submit a request to be given access to any classified records which they originated, reviewed, signed, or received while serving in that capacity. Such appointees may also request approval for a research associate but there is no entitlement to such enlargement of access and the decision in this regard shall be in the sole discretion of the Agency. Requests from appointees shall be in writing to the Coordinator and shall identify the records of interest.

32 CFR Section 1909.12: Designations of authority to hear requests.
The Deputy Director for Administration has designated the Coordinator, the Agency Release Panel, and the Historical Records Policy Board, established pursuant to 32 CFR 1900.41, as the Agency authorities to decide requests for historical and former Presidential appointee access under Executive Order 12958 (or successor Orders) and these regulations.

32 CFR Section 1909.13: Receipt, recording, and tasking.
The Information and Privacy Coordinator shall within ten (10) days record each request for historical access received under this Part, acknowledge receipt to the requester in writing and take the following action:

(a) Compliance with general requirements.

The Coordinator shall review each request under this part and determine whether it meets the general requirements as set forth in 32 CFR 1909.11; if it does not, the Coordinator shall so notify the requester and explain the legal basis for this decision.

(b) Action on requests meeting general requirements.

For requests which meet the requirements of 32 CFR 1909.11, the Coordinator shall thereafter task the D/CSI, the originator(s) of the materials for which access is sought, and other interested parties. Additional taskings, as required during the review process, shall be accomplished within ten (10) days of notification.

32 CFR Section 1909.14: Determinations by tasked officials.

(a) Required determinations.

The tasked parties as specified below shall respond in writing to the Coordinator with recommended findings to the following issues:
(1) That a serious professional or scholarly research project by the requester is contemplated (by D/CSI);
(2) That such access is clearly consistent with the interests of national security (by originator and interested party, if any);
(3) That a non-disclosure agreement has been or will be executed by the requester (or research associate, if any) and other appropriate steps have been taken to assure that classified information will not be disclosed or otherwise compromised (by Director of Personnel Security and representative of the Office of General Counsel);
(4) That a pre-publication agreement has been or will be executed by the requester (or research associate, if any) which provides for a review of notes and any resulting manuscript (by Director of Personnel Security and representative of the Office of General Counsel);
(5) That the information requested is reasonably accessible and can be located and compiled with a reasonable effort (by D/CSI and originator);
(6) That it is reasonably expected that substantial and substantive government documents and/or information will be amenable to declassification and release and/or publication (by D/CSI and originator);
(7) That sufficient resources are available for the administrative support of the researcher given current mission requirements (by D/CSI and originator); and,
(8) That the request cannot be satisfied to the same extent through requests for access to reasonably described records under the Freedom of Information Act or the mandatory declassification review provisions of Executive Order 12958 (by Coordinator, D/CSI and originator).

(b) Time.

These responses shall be provided expeditiously on a “first-in, first-out” basis taking into account the business requirements of the tasked offices and consistent with the information rights of members of the general public under the Freedom of Information Act and the Privacy Act. The Agency will utilize its best efforts to complete action on requests under this part within thirty (30) days of date of receipt.

32 CFR Section 1909.15: Action by hearing authority.

Action by Agency Release Panel.

The Coordinator, in his or her capacity as Executive Secretary of the Agency Release Panel, shall place historical access requests ready for adjudication on the agenda at the next occurring meeting of the Agency Release Panel. The Executive Secretary shall provide a summation memorandum for consideration of the members, the complete record of the request consisting of the request and the findings of the tasked parties. The Panel shall meet and decide requests sitting as a committee of the whole on the basis of the eight factors enumerated at 32 CFR 1909.14(a). Decisions are by majority vote of those present at a meeting and shall
be based on the written record and their deliberations; no personal appearances shall be permitted without the express permission of the Panel.

32 CFR Section 1909.16: Action by appeal authority.
In any cases of divided vote by the ARP, any member of that body is authorized to refer the request to the CIA Historical Records Policy Board which acts as the senior corporate board for the Agency. The record compiled (the request, the memoranda filed by the originator and interested parties, and the previous decision(s)) as well as any memorandum of law or policy the referent desires to be considered, shall be certified by the Executive Secretary of the Agency Release Panel and shall constitute the official record of the proceedings and must be included in any subsequent filings. In such cases, the factors to be determined as specified in 32 CFR 1909.14(a) will be considered by the Board de novo and that decision shall be final.

32 CFR Section 1909.17: Notification of decision.
The Coordinator shall inform the requester of the decision of the Agency Release Panel or the Historical Records Policy Board within ten (10) days of the decision and, if favorable, shall manage the access for such period as deemed required but in no event for more than two (2) years unless renewed by the Panel or Board in accordance with the requirements of 32 CFR 1909.14(a).

32 CFR Section 1909.18: Termination of access.
The Coordinator shall cancel any authorization whenever the Director of Personnel Security cancels the security clearance of a requester (or research associate, if any) or whenever the Agency Release Panel determines that continued access would not be in compliance with one or more of the requirements of 32 CFR 1909.14(a).
32 CFR PART 1910—DEBARMENT AND SUSPENSION PROCEDURES

1910.1: General.

Authority:

The Central Intelligence Agency (CIA), in accordance with its authorities under the Central Intelligence Agency Act of 1949, as amended, and the National Security Act of 1947, as amended, has an established debarment and suspension process in accordance with subpart 9.402(d) of the Federal Acquisition Regulation (FAR). This process and the causes for debarment and suspension are consistent with those found in FAR 9.406 and 9.407. The rights of CIA contractors in all matters involving debarment and suspension are hereby governed by the provisions of subpart 9.4 of the FAR.

[69 FR 63064, Oct. 29, 2004]
32 CFR CHAPTER XX—INFORMATION SECURITY
OVERSIGHT OFFICE, NATIONAL ARCHIVES AND
RECORDS ADMINISTRATION

- Part 2000: Administrative procedures [Reserved]
- Part 2001: Classified national security information
- Part 2003: [Reserved]

32 CFR PART 2000—ADMINISTRATIVE PROCEDURES
[RESERVED]
Subpart A—Scope of Part
  o 2001.1: Purpose and scope.

Subpart B—Classification
  o 2001.10: Classification standards.
  o 2001.11: Original classification authority.
  o 2001.12: Duration of classification.
  o 2001.14: Classification challenges.
  o 2001.15: Classification guides.

Subpart C—Identification and Markings
  o 2001.23: Classification marking in the electronic environment.
  o 2001.24: Additional requirements.
  o 2001.26: Automatic declassification exemption markings.

Subpart D—Declassification
  o 2001.30: Automatic declassification.
  o 2001.31: Systematic declassification review.
  o 2001.32: Declassification guides.
  o 2001.33: Mandatory review for declassification.
  o 2001.34: Referrals.
  o 2001.35: Discretionary declassification.
  o 2001.36: Classified information in the custody of private organizations or individuals.
  o 2001.37: Assistance to the Department of State.

Subpart E—Safeguarding
  o 2001.43: Storage.
  o 2001.44: Reciprocity of use and inspection of facilities.
2001.48: Loss, possible compromise, or unauthorized disclosure.
2001.49: Special access programs.
2001.50: Telecommunications, automated information systems, and network security.
2001.53: Open storage areas.

Subpart F—Self-Inspections

Subpart G—Security Education and Training
2001.70: General.

Subpart H—Standard Forms

Subpart I—Reporting and Definitions
2001.90: Agency annual reporting requirements.
2001.91: Other agency reporting requirements.

Authority:
Sections 5.1(a) and (b), E.O. 13526, (75 FR 707, January 5, 2010).

Source:
75 FR 37254, June 28, 2010, unless otherwise noted.
SUBPART A—Scope of Part


(a) This part is issued under Executive Order. (E.O.) 13526, Classified National Security Information (the Order).

Section 5 of the Order provides that the Director of the Information Security Oversight Office (ISOO) shall develop and issue such directives as are necessary to implement the Order.

(b) The Order provides that these directives are binding on agencies. Section 6.1(a) of the Order defines “agency” to mean any “Executive agency” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) For the convenience of the user, the following table provides references between the sections contained in this part and the relevant sections of the Order.

<table>
<thead>
<tr>
<th>CFR section</th>
<th>Related section of E.O. 13526</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001.10 Classification standards</td>
<td>1.1, 1.4</td>
</tr>
<tr>
<td>2001.11 Original classification authority</td>
<td>1.3</td>
</tr>
<tr>
<td>2001.12 Duration of classification</td>
<td>1.5</td>
</tr>
<tr>
<td>2001.13 Classification prohibitions and limitations</td>
<td>1.7</td>
</tr>
<tr>
<td>2001.14 Classification challenges</td>
<td>1.8</td>
</tr>
<tr>
<td>2001.15 Classification guides</td>
<td>2.2</td>
</tr>
<tr>
<td>2001.16 Fundamental classification guidance review</td>
<td>1.9</td>
</tr>
<tr>
<td>2001.20 General</td>
<td>1.6</td>
</tr>
</tbody>
</table>
2001.21 Original classification
1.6(a)

2001.22 Derivative classification
2.1

2001.23 Classification marking in the electronic environment
1.6

2001.24 Additional requirements
1.6

2001.25 Declassification markings
1.5, 1.6, 3.3

2001.26 Automatic declassification exemption markings
3.3

2001.30 Automatic declassification
3.3, 3.7

2001.31 Systematic declassification review
3.4

2001.32 Declassification guides
3.3, 3.7

2001.33 Mandatory review for declassification
3.5, 3.6

2001.34 Referrals
3.3, 3.6, 3.7

2001.35 Discretionary declassification
3.1

2001.36 Classified information in the custody of private organizations or individuals
none

2001.37 Assistance to the Department of State
none

2001.40 General
4.1

Page 1104
2001.41 Responsibilities of holders
4.1

2001.42 Standards for security equipment
4.1

2001.43 Storage
4.1

2001.44 Reciprocity of use and inspection of facilities
4.1

2001.45 Information controls
4.1, 4.2

2001.46 Transmission
4.1, 4.2

2001.47 Destruction
4.1, 4.2

2001.48 Loss, possible compromise, or unauthorized disclosure
4.1, 4.2

2001.49 Special access programs
4.3

2001.50 Telecommunications, automated information systems, and network security
4.1, 4.2

2001.51 Technical security
4.1

2001.52 Emergency authority
4.2

2001.53 Open storage areas
4.1

2001.54 Foreign government information
4.1

2001.55 Foreign disclosure of classified information
4.1(i)(2)
2001.60 Self-Inspections, General
5.4

2001.70 Security Education and Training, General
5.4

2001.71 Coverage
1.3(d), 2.1(d), 3.7(b), 4.1(b), 5.4(d)(3)

2001.80 Prescribed standard forms
5.2(b)(7)

2001.90 Agency annual reporting requirements
1.3(c), 5.2(b)(4), 5.4(d)(4), 5.4(d)(8)

2001.91 Other agency reporting requirements
1.3(d), 1.7(c)(3), 1.9(d), 2.1(d), 5.5

2001.92 Definitions
6.1
SUBPART B—Classification

32 CFR Section 2001.10: Classification standards.

Identifying or describing damage to the national security.

Section 1.1(a) of the Order specifies the conditions that must be met when making classification decisions. Section 1.4 specifies that information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security. There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand pursuant to the Order or law.


(a) General.

Agencies shall establish a training program for original classifiers in accordance with subpart G of this part.

(b) Requests for original classification authority.

Agencies not possessing such authority shall forward requests to the Director of ISOO. The agency head must make the request and shall provide a specific justification of the need for this authority. The Director of ISOO shall forward the request, along with the Director’s recommendation, to the President through the National Security Advisor within 30 days. Agencies wishing to increase their assigned level of original classification authority shall forward requests in accordance with the procedures of this paragraph.

(c) Reporting delegations of original classification authority.

All delegations of original classification authority shall be reported to the Director of ISOO. This can be accomplished by an initial submission followed by updates on a frequency determined by the senior agency official, but at least annually.


(a) Determining duration of classification for information originally classified under the Order

(1) Establishing duration of classification.
Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, an original classification
authority shall follow the sequence listed in paragraphs (a)(1)(i), (ii), and (iii) of this section when determining the duration of classification for information originally classified under this Order.

(i) The original classification authority shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

(ii) If unable to determine a date or event of less than 10 years, the original classification authority shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

(iii) If unable to determine a date or event of 10 years, the original classification authority shall assign a declassification date not to exceed 25 years from the date of the original classification decision.

(2) Duration of classification of special categories of information.
The only exceptions to the sequence in paragraph (a)(1) of this section are as follows:

(i) If an original classification authority is classifying information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, the duration shall be up to 75 years and shall be designated with the following marking, “50X1-HUM;” or

(ii) If an original classification authority is classifying information that should clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, the duration shall be up to 75 years and shall be designated with the following marking, “50X2-WMD.”

(b) Extending duration of classification for information classified under the Order.

Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

(1) If the date or event assigned by the original classification authority has not passed, an original classification authority with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origin of the record.

(2) If the date or event assigned by the original classification authority has passed, an original classification authority with jurisdiction over the information may reclassify the information in accordance with the Order and this Directive only if it meets the standards for classification under sections 1.1 and 1.5 of the Order as well as section 3.3 of the Order, if appropriate.

(3) In all cases, when extending the duration of classification, the original classification authority must:

(i) Be an original classification authority with jurisdiction over the information;
(ii) Ensure that the information continues to meet the standards for classification under the Order; and
(iii) Make reasonable attempts to notify all known holders of the information.

(c) Duration of information classified under prior orders

(1) Specific date or event.
Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. If the specific date or event has not passed, an original classification authority with jurisdiction over the information may extend the duration in accordance with the requirements of paragraph (b) of this section. If the date or event assigned by the original classification authority has passed, an original classification authority with jurisdiction over the information may only reclassify information in accordance with the standards and procedures under the Order and this Directive. If the information is contained in records determined to be permanently valuable, and the prescribed date or event will take place more than 25 years from the date of origin of the document, the declassification of the information will instead be subject to section 3.3 of the Order.

(2) Indefinite duration of classification.
For information marked with X1, X2, X3, X4, X5, X6, X7, or X8; “Originating Agency’s Determination Required” or its acronym “OADR,” “Manual Review” or its acronym “MR,” “DCI Only;” “DNI Only;” and any other marking indicating an indefinite duration of classification under a prior order; or in those cases where a document is missing a required declassification instruction or the instruction is not complete:
(i) A declassification authority, as defined in section 3.1(b) of the Order, may declassify it;
(ii) An original classification authority with jurisdiction over the information may re-mark the information to establish a duration of classification of no more than 25 years from the date of origin of the document, consistent with the requirements for information originally classified under the Order, as provided in paragraph (a) of this section; or
(iii) Unless declassified earlier, such information contained in records determined to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.3 of the Order.

(3) Release of imagery acquired by space-based intelligence reconnaissance systems.
The duration of classification of imagery as defined in E.O. 12951, Release of Imagery Acquired by Space-Based Intelligence Reconnaissance Systems, that is otherwise marked with an indefinite duration, such as “DCI Only” or “DNI Only,” shall be established by the Director of National Intelligence in accordance with E.O. 12951 and consistent with E.O. 13526. Any such information shall be remarked in accordance with instructions prescribed by the Director of National Intelligence.

(a) Declassification without proper authority.

Classified information that has been declassified without proper authority, as determined by an original classification authority with jurisdiction over the information, remains classified and administrative action shall be taken to restore markings and controls, as appropriate. All such determinations shall be reported to the senior agency official who shall promptly provide a written report to the Director of ISOO.

(1) If the information at issue is in records in the physical and legal custody of the National Archives and Records Administration (NARA) and has been made available to the public, the original classification authority with jurisdiction over the information shall, as part of determining whether the restoration of markings and controls is appropriate, consider whether the removal of the information from public purview will significantly mitigate the harm to national security or otherwise draw undue attention to the information at issue. Written notification, classified when appropriate under the Order, shall be made to the Archivist, which shall include a description of the record(s) at issue, the elements of information that are classified, the duration of classification, and the specific authority for continued classification. If the information at issue is more than 25 years of age and the Archivist does not agree with the decision, the information shall nonetheless be temporarily withdrawn from public access and shall be referred to the Director of ISOO for resolution in collaboration with affected parties.

(b) Reclassification after declassification and release to the public under proper authority.

In making the decision to reclassify information that has been declassified and released to the public under proper authority, the agency head must approve, in writing, a determination on a document-by-document basis that the reclassification is required to prevent significant and demonstrable damage to the national security. As part of making such a determination, the following shall apply:

(1) The information must be reasonably recoverable without bringing undue attention to the information which means that:

(i) Most individual recipients or holders are known and can be contacted and all instances of the information to be reclassified will not be more widely disseminated;

(ii) If the information has been made available to the public via a means such as Government archives or reading room, consideration is given to length of time the record has been available to the public, the extent to which the record has been accessed for research, and the extent to which the record and/or classified information at issue has been copied, referenced, or publicized; and
(iii) If the information has been made available to the public via electronic means such as the internet, consideration is given as to the number of times the information was accessed, the form of access, and whether the information at issue has been copied, referenced, or publicized.

(2) If the reclassification concerns a record in the physical custody of NARA and has been available for public use, reclassification requires notification to the Archivist and approval by the Director of ISOO.

(3) Any recipients or holders of the reclassified information who have current security clearances shall be appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holders who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information that they have had access to, their obligation not to disclose the information, and be requested to sign an acknowledgement of this briefing.

(4) The reclassified information must be appropriately marked in accordance with section 2001.24(l) and safeguarded. The markings should include the authority for and the date of the reclassification action.

(5) Once the reclassification action has occurred, it must be reported to the National Security Advisor and to the Director of ISOO by the agency head or senior agency official within 30 days. The notification must include details concerning paragraphs (b)(1) and (3) of this section.

(c) Classification by compilation.

A determination that information is classified through the compilation of unclassified information is a derivative classification action based upon existing original classification guidance. If the compilation of unclassified information reveals a new aspect of information that meets the criteria for classification, it shall be referred to an original classification authority with jurisdiction over the information to make an original classification decision.


(a) Challenging classification.

Authorized holders, including authorized holders outside the classifying agency, who want to challenge the classification status of information shall present such challenges to an original classification authority with jurisdiction over the information. An authorized holder is any individual who has been granted access to specific classified information in accordance with the provisions of the Order to include the special conditions set forth in section 4.1(h) of the Order. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level.

(b) Agency procedures.
Because the Order encourages authorized holders to challenge classification as a means for promoting proper and thoughtful classification actions, agencies shall ensure that no retribution is taken against any authorized holders bringing such a challenge in good faith.

Agencies shall establish a system for processing, tracking and recording formal classification challenges made by authorized holders. Agencies shall consider classification challenges separately from Freedom of Information Act or other access requests, and shall not process such challenges in turn with pending access requests.

The agency shall provide an initial written response to a challenge within 60 days. If the agency is unable to respond to the challenge within 60 days, the agency must acknowledge the challenge in writing, and provide a date by which the agency will respond. The acknowledgment must include a statement that if no agency response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (Panel) for a decision. The challenger may also forward the challenge to the Panel if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal. Agency responses to those challenges it denies shall include the challenger's appeal rights to the Panel.

Whenever an agency receives a classification challenge to information that has been the subject of a challenge within the past two years, or that is the subject of pending litigation, the agency is not required to process the challenge beyond informing the challenger of this fact and of the challenger's appeal rights, if any.

(c) Additional considerations.

Challengers and agencies shall attempt to keep all challenges, appeals and responses unclassified. However, classified information contained in a challenge, an agency response, or an appeal shall be handled and protected in accordance with the Order and this Directive. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be encouraged as a means of holding down the number of formal challenges and to ensure the integrity of the classification process.

32 CFR Section 2001.15: Classification guides.

(a) Preparation of classification guides.

Originators of classification guides are encouraged to consult users of guides for input when developing or updating guides. When possible, originators of classification guides are encouraged to communicate within their agencies and with other agencies that are developing guidelines for similar activities to ensure
the consistency and uniformity of classification decisions. Each agency shall maintain a list of its classification guides in use.

(b) General content of classification guides.

Classification guides shall, at a minimum:

(1) Identify the subject matter of the classification guide;
(2) Identify the original classification authority by name and position, or personal identifier;
(3) Identify an agency point-of-contact or points-of-contact for questions regarding the classification guide;
(4) Provide the date of issuance or last review;
(5) State precisely the elements of information to be protected;
(6) State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;
(7) State, when applicable, special handling caveats;
(8) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.4 of the Order; and
(9) Prescribe a specific date or event for declassification, the marking “50X1-HUM” or “50X2-WMD” as appropriate, or one or more of the exemption codes listed in 2001.26(a)(2), provided that:

(i) The exemption has been approved by the Panel under section 3.3(j) of the Order;
(ii) The Panel is notified of the intent to take such actions for specific information in advance of approval and the information remains in active use; and
(iii) The exemption code is accompanied with a declassification date or event that has been approved by the Panel.

(c) Dissemination of classification guides.

Classification guides shall be disseminated as necessary to ensure the proper and uniform derivative classification of information.

(d) Reviewing and updating classification guides.

(1) Agencies shall incorporate original classification decisions into classification guides as soon as practicable.
(2) Originators of classification guides are encouraged to consult the users of guides and other subject matter experts when reviewing or updating guides. Also, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide.

(a) Performance of fundamental classification guidance reviews.

An initial fundamental classification guidance review shall be completed by every agency with original classification authority and which authors security classification guides no later than June 27, 2012. Agencies shall conduct fundamental classification guidance reviews on a periodic basis thereafter. The frequency of the reviews shall be determined by each agency considering factors such as the number of classification guides and the volume and type of information they cover. However, a review shall be conducted at least once every five years.

(b) Coverage of reviews.

At a minimum, the fundamental classification guidance review shall focus on:

(1) Evaluation of content.
   (i) Determining if the guidance conforms to current operational and technical circumstances; and
   (ii) Determining if the guidance meets the standards for classification under section 1.4 of the Order and an assessment of likely damage under section 1.2 of the Order; and

(2) Evaluation of use:
   (i) Determining if the dissemination and availability of the guidance is appropriate, timely, and effective; and
   (ii) An examination of recent classification decisions that focuses on ensuring that classification decisions reflect the intent of the guidance as to what is classified, the appropriate level, the duration, and associated markings.

(c) Participation in reviews.

The agency head or senior agency official shall direct the conduct of a fundamental classification guidance review and shall ensure the appropriate agency subject matter experts participate to obtain the broadest possible range of perspectives. To the extent practicable, input should also be obtained from external subject matter experts and external users of the reviewing agency's classification guidance and decisions.

(d) Reports on results.

Agency heads shall provide a detailed report summarizing the results of each classification guidance review to ISOO and release an unclassified version to the public except when the existence of the guide or program is itself classified.
SUBPART C—Identification and Markings


A uniform security classification system requires that standard markings or other indicia be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.


(a) Primary markings.

At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

(1) Classification authority.
The name and position, or personal identifier, of the original classification authority shall appear on the “Classified By” line. An example might appear as:

Classified By: David Smith, Chief, Division 5
or
Classified By: ID#IMNO1

(2) Agency and office of origin.
If not otherwise evident, the agency and office of origin shall be identified and follow the name on the “Classified By” line. An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration.

(3) Reason for classification.
The original classification authority shall identify the reason(s) for the decision to classify. The original classification authority shall include on the “Reason” line the number 1.4 plus the letter(s) that corresponds to that classification category in section 1.4 of the Order.
(i) These categories, as they appear in the Order, are as follows:
(A) Military plans, weapons systems, or operations;
(B) Foreign government information;
(C) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;
(D) Foreign relations or foreign activities of the United States, including confidential sources;
(E) Scientific, technological, or economic matters relating to the national security;
(F) United States Government programs for safeguarding nuclear materials or facilities;
(G) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
(H) The development, production, or use of weapons of mass destruction.

(ii) An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration Reason: 1.4(g)

(4) Declassification instructions.
The duration of the original classification decision shall be placed on the “Declassify On” line. When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD. Events must be reasonably definite and foreseeable. The original classification authority will apply one of the following instructions:
(i) A date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which is equal to or less than 10 years from the date of the original decision. The duration of classification would be marked as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20201014 or
Declassify On: Completion of Operation

(ii) A date not to exceed 25 years from the date of the original decision. For example, on a document that contains information classified on October 10, 2010, apply a date up to 25 years on the “Declassify On” line:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20351010

(iii) If the classified information should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source,
(iv) If the classified information should clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, no date or event is required and the marking “50X2-WMD” shall be used in the “Declassify On” line.

(b) Overall marking.

The highest level of classification is determined by the highest level of any one portion within the document and shall appear in a way that will distinguish it clearly from the informational text.

(1) Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked “Secret” and other information marked “Confidential,” the overall marking would be “Secret.”

(3) Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation “Unclassified” when it is applicable, or with the highest overall classification of the document.

(c) Portion marking.

Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which portions are unclassified by placing a parenthetical symbol immediately preceding the portion to which it applies.

(1) To indicate the appropriate classification level, the symbols “(TS)” for Top Secret, “(S)” for Secret, and “(C)” for Confidential will be used.

(2) Portions which do not meet the standards of the Order for classification shall be marked with “(U)” for Unclassified.

(3) In cases where portions are segmented such as paragraphs, sub-paragraphs, bullets, and sub-bullets and the classification level is the same throughout, it is sufficient to put only one portion marking at the beginning of the main paragraph or main bullet. If there are different levels of classification among these segments, then all segments shall be portion marked separately in order to avoid over-classification of any one segment. If the information contained in a sub-paragraph or sub-bullet is a higher level of classification than its parent paragraph or parent bullet, this does not make the parent paragraph or parent bullet classified at that same level. Each portion shall reflect the classification level of that individual portion and not any other portions. At the same time, any
portion, no matter what its status, is still capable of determining the overall classification of the document.

(d) Dissemination control and handling markings.

Many agencies require additional control and handling markings that supplement the overall classification markings. See § 2001.24(j) for specific guidance.

(e) Date of origin of document.

The date of origin of the document shall be indicated in a manner that is immediately apparent.


(a) General.

Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2001.20 and § 2001.21, except as provided in this section. Information for these markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

(b) Identity of persons who apply derivative classification markings.

Derivative classifiers shall be identified by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document. If not otherwise evident, the agency and office of origin shall be identified and follow the name on the “Classified By” line. An example might appear as:

Classified By: Peggy Jones, Lead Analyst, Research and Analysis Division or Classified By: ID # IMN01

(c) Source of derivative classification.

(1) The derivative classifier shall concisely identify the source document or the classification guide on the “Derived From” line, including the agency and, where available, the office of origin, and the date of the source or guide. An example might appear as:

Derived From: Memo, “Funding Problems,” October 20, 2008, Office of Administration, Department of Good Works or

Derived From: CG No. 1, Department of Good Works, dated October 20, 2008
(i) When a document is classified derivatively on the basis of more than one source document or classification guide, the “Derived From” line shall appear as:

Derived From: Multiple Sources

(ii) The derivative classifier shall include a listing of the source materials on, or attached to, each derivatively classified document. A document derivatively classified on the basis of a source document that is itself marked “Multiple Sources” shall cite the source document on its “Derived From” line rather than the term “Multiple Sources.” An example might appear as:

Derived From: Report entitled, “New Weapons,” dated October 20, 2009, Department of Good Works, Office of Administration

(d) Reason for classification.

The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not transferred in a derivative classification action.

(e) Declassification instructions.

(1) The derivative classifier shall carry forward the instructions on the “Declassify On” line from the source document to the derivative document, or the duration instruction from the classification or declassification guide, unless it contains one of the declassification instructions as listed in paragraph (e)(3) of this section. If the source document is missing the declassification instruction, then a calculated date of 25 years from the date of the source document (if available) or the current date (if the source document date is not available) shall be carried forward by the derivative classifier.

(2) When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the “Declassify On” line shall reflect the longest duration of any of its sources.

(3) When a document is classified derivatively either from a source document(s) or a classification guide that contains one of the following declassification instructions, “Originating Agency's Determination Required,” “OADR,” or “Manual Review,” “MR,” or any of the exemption markings X1, X2, X3, X4, X5, X6, X7, and X8, the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document’s date or event to be placed in the “Declassify On” line. If a document is marked with the declassification instructions “DCI Only” or “DNI Only” and does not contain information described in E.O. 12951, “Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems,” the derivative classifier shall calculate a date that is 25 years from the
date of the source document when determining a derivative document’s date or event to be placed in the “Declassify On” line.

(ii) If a document is marked with “DCI Only” or “DNI Only” and the information is subject to E.O. 12951, the derivative classifier shall use a date or event as prescribed by the Director of National Intelligence.

(4) When determining the most restrictive declassification instruction among multiple source documents, adhere to the following hierarchy for determining the declassification instructions for the “Declassify On” line:

(i) 50X1-HUM or 50X2-WMD, or an ISOO-approved designator reflecting the Panel approval for classification beyond 50 years in accordance with section 3.3(h)(2) of the Order;

(ii) 25X1 through 25X9, with a date or event;

(iii) A specific declassification date or event within 25 years;

(iv) Absent guidance from an original classification authority with jurisdiction over the information, a calculated 25-year date from the date of the source document.

(5) When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD.

(f) Overall marking.

The derivative classifier shall conspicuously mark the classified document with the highest level of classification of information included in the document, as provided in § 2001.21(b).

(g) Portion marking.

Each portion of a derivatively classified document shall be marked immediately preceding the portion to which it applies, in accordance with its source, and as provided in § 2001.21(c).

(h) Dissemination control and handling markings.

Many agencies require additional control and handling markings that supplement the overall classification markings. See § 2001.24(j) for specific guidance.

(i) Date of origin of document.

The date of origin of the document shall be indicated in a manner that is immediately apparent.

32 CFR Section 2001.23: Classification marking in the electronic environment.

(a) General.
Classified national security information in the electronic environment shall be:
(1) Subject to all requirements of the Order.
(2) Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, “Classified By,” “Derived From,” “Reason” for classification (originally classified information only), and “Declassify On.”
(3) Marked with proper classification markings when appearing in an electronic output (e.g., database query) in which users of the information will need to be alerted to the classification status of the information.
(4) Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in this manner, a warning shall be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information.
(5) Prohibited from use as source of derivative classification if it is dynamic in nature (e.g., wikis and blogs) and where information is not marked in accordance with the Order.

(b) Markings on classified e-mail messages.

(1) E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail shall reflect the classification of the header and body of the message. This includes the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail. A single linear text string showing the overall classification and markings shall be included in the first line of text and at the end of the body of the message after the signature block.
(2) Classified e-mail shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A text portion containing a uniform resource locator (URL) or reference (i.e., link) to another document shall be portion marked based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.
(3) A classified signature block shall be portion marked to reflect the highest classification level markings of the information contained in the signature block itself.
(4) Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.
(5) For a classified e-mail, the classification authority block shall be placed after the signature block, but before the overall classification marking string at the end.
of the e-mail. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) When forwarding or replying to an e-mail, individuals shall ensure that, in addition to the markings required for the content of the reply or forward e-mail itself, the markings shall reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

(c) Marking Web pages with classified content.

(1) Web pages shall be classified and marked on their own content regardless of the classification of the pages to which they link. Any presentation of information to which the web materials link shall also be marked based on its own content.

(2) The overall classification marking string for every web page shall reflect the overall classification markings (and any dissemination control or handling markings) for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

(3) If any graphical representation is utilized, a text equivalent of the overall classification marking string shall be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allows for the use of text translators.

(4) Classified Web pages shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another document shall be portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

(5) Classified Web pages shall include the classification authority block on either the top or bottom of the page. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) Electronic media files such as video, audio, images, or slides shall carry the overall classification and classification authority block, unless the addition of such information would render them inoperable. In such cases, another procedure shall be used to ensure recipients are aware of the classification status of the information and the declassification instructions.

(d) Marking classified URLs.

URLs provide unique addresses in the electronic environment for web content and shall be portion marked based on the classification of the content of the URL itself. The URL shall not be portion marked to reflect the classification of the content to which it points. URLs shall be developed at an unclassified level whenever possible. When a URL is classified, a classification portion mark shall be used in the text of the URL string in a way that does not make the URL inoperable to identify the URL as a classified portion in any textual references to that URL. An example may appear as:
(e) Marking classified dynamic documents and relational databases.  
(1) A dynamic page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification levels of information returned may vary depending upon the specific request.  
(2) If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings shall be applied to and displayed on the document. If such a mechanism does not exist, the default should be the highest level of information in the database and a warning shall be applied at the top of each page of the document. Such content shall not be used as a basis for derivative classification. An example of such an applied warning may appear as:

This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification; refer instead to the pertinent classification guide(s).

(3) This will alert the users of the information that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned. Users shall be encouraged to make further inquiries concerning the status of individual elements in order to avoid unnecessary classification and/or impediments to information sharing. Resources such as classification guides and points of contact shall be established to assist with these inquiries.

(4) Users developing a document based on query results from a database must properly mark the document in accordance with § 2001.22. If there is doubt about the correct markings, users should contact the database originating agency for guidance.

(f) Marking classified bulletin board postings and blogs.

(1) A blog, an abbreviation of the term “web log,” is a Web site consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual as in a journal or by many individuals. While the content of the overall blog is dynamic, entries are generally static in nature.  
(2) The overall classification marking string for every bulletin board or blog shall reflect the overall classification markings for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable.
(3) Subject lines of bulletin board postings, blog entries, or comments shall be portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.

(4) The overall classification marking string for the bulletin board posting, blog entry, or comment shall reflect the classification markings for the subject line, the text of the posting, and any other information in the posting. These strings shall be entered manually or utilizing an electronic classification tool in the first line of text and at the end of the body of the posting. These strings may appear as single linear text.

(5) Bulletin board postings, blog entries, or comments shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(g) Marking classified wikis.

(1) Initial wiki submissions shall include the overall classification marking string, portion marking, and the classification authority block string in the same manner as mentioned above for bulletin boards and blogs. All of these strings may appear as single line text.

(2) When users modify existing entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information. Systems shall provide a means to log the identity of each user, the changes made, and the time and date of each change.

(3) Wiki articles and entries shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(h) Instant messaging, chat, and chat rooms.

(1) Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing shall be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block string shall also appear.

(2) Chat rooms shall display system-high overall classification markings and shall contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block.

(i) Attached files.

When files are attached to another electronic message or document, the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked in accordance with § 2001.24(b).

(a) Marking prohibitions.

Markings other than “Top Secret,” “Secret,” and “Confidential” shall not be used to identify classified national security information.

(b) Transmittal documents.

A transmittal document shall indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal shall also include conspicuously on its face the following or similar instructions, as appropriate:
Unclassified When Classified Enclosure Removed or
Upon Removal of Attachments, This Document is (Classification Level)

(c) Foreign government information.

Unless otherwise evident, documents that contain foreign government information should include the marking, “This Document Contains (indicate country of origin) Information.” Agencies may also require that the portions of the documents that contain the foreign government information be marked to indicate the government and classification level, using accepted country code standards, e.g., “(Country code—C).” If the identity of the specific government must be concealed, the document shall be marked, “This Document Contains Foreign Government Information,” and pertinent portions shall be marked “FGI” together with the classification level, e.g., “(FGI-C).” In such cases, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions. If the fact that information is foreign government information must be concealed, the markings described in this paragraph shall not be used and the document shall be marked as if it were wholly of U.S. origin. When classified records are transferred to NARA for storage or archival purposes, the accompanying documentation shall, at a minimum, identify the boxes that contain foreign government information.

(d) Working papers.

A working paper is defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, and if otherwise
appropriate, destroyed when no longer needed. When any of the following conditions applies, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

1. Released by the originator outside the originating activity;
2. Retained more than 180 days from the date of origin; or
3.Filed permanently.

(e) Other material.

Bulky material, equipment, and facilities, etc., shall be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding must be maintained in the appropriate security facility.

(f) Unmarked materials.

Information contained in unmarked records, or presidential or related materials, and which pertains to the national defense or foreign relations of the United States, created, maintained, and protected as classified information under prior orders shall continue to be treated as classified information under the Order, and is subject to its provisions regarding declassification.

(g) Classification by compilation/aggregation.

Compilation of items that are individually unclassified may be classified if the compiled information meets the standards established in section 1.2 of the Order and reveals an additional association or relationship, as determined by the original classification authority. Any unclassified portions will be portion marked (U), while the overall markings will reflect the classification of the compiled information even if all the portions are marked (U). In any such situation, clear instructions must appear with the compiled information as to the circumstances under which the individual portions constitute a classified compilation, and when they do not.

(h) Commingling of Restricted Data (RD) and Formerly Restricted Data (FRD) with information classified under the Order.

1. To the extent practicable, the commingling in the same document of RD or FRD with information classified under the Order should be avoided. When it is not practicable to avoid such commingling, the marking requirements in the Order and this Directive, as well as the marking requirements in 10 CFR part 1045, Nuclear Classification and Declassification, must be followed.
2. Automatic declassification of documents containing RD or FRD is prohibited. Documents marked as containing RD or FRD are excluded from the automatic declassification provisions of the Order until the RD or FRD designation is
properly removed by the Department of Energy. When the Department of Energy
determines that an RD or FRD designation may be removed, any remaining
information classified under the Order must be referred to the appropriate
agency in accordance with the declassification provisions of the Order and this
Directive.

(3) For commingled documents, the “Declassify On” line required by the Order
and this Directive shall not include a declassification date or event and shall
instead be annotated with “Not Applicable (or N/A) to RD/FRD portions” and
“See source list for NSI portions.” The source list, as described in §
2001.22(c)(1)(ii), shall include the declassification instruction for each of the
source documents classified under the Order and shall not appear on the front
page of the document.

(4) If an RD or FRD portion is extracted for use in a new document, the
requirements of 10 CFR part 1045 must be followed.

(5) If a portion classified under the Order is extracted for use in a new document,
the requirements of the Order and this Directive must be followed. The
declassification date for the extracted portion shall be determined by using the
source list required by § 2001.22(c)(1)(ii), the pertinent classification guide, or
consultation with the original classification authority with jurisdiction for the
information. However, if a commingled document is not portion marked, it shall
not be used as a source for a derivatively classified document.

(6) If a commingled document is not portion marked based on appropriate
authority, annotating the source list with the declassification instructions and
including the “Declassify on” line in accordance with paragraph (h)(3) of this
section are not required. The lack of declassification instructions does not
eliminate the requirement to process commingled documents for declassification
in accordance with the Order, this Directive, the Atomic Energy Act, or 10 CFR
part 1045 when they are requested under statute or the Order.

(i) Transclassified Foreign Nuclear Information (TFNI).

(1) As permitted under 42 U.S.C. 2162(e), the Department of Energy shall
remove from the Restricted Data category such information concerning the
atomic energy programs of other nations as the Secretary of Energy and the
Director of National Intelligence jointly determine to be necessary to carry out
the provisions of 50 U.S.C. 403 and 403-1 and safeguarded under applicable
Executive orders as “National Security Information” under a process called
transclassification.

(2) When Restricted Data information is transclassified and is safeguarded as
“National Security Information,” it shall be handled, protected, and classified in
conformity with the provisions of the Order and this Directive. Such information
shall be labeled as “TFNI” and with any additional identifiers prescribed by the
Department of Energy. The label “TFNI” shall be included on documents to
indicate the information's transclassification from the Restricted Data category
and its declassification process governed by the Secretary of Energy under the
Atomic Energy Act.
(3) Automatic declassification of documents containing TFNI is prohibited. Documents marked as containing TFNI are excluded from the automatic declassification provisions of the Order until the TFNI designation is properly removed by the Department of Energy. When the Department of Energy determines that a TFNI designation may be removed, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification provisions of the Order and this Directive.

(j) Approved dissemination control and handling markings.

(1) Dissemination control and handling markings identify the expansion or limitation on the distribution of the information. These markings are in addition to, and separate from, the level of classification.
(2) Only those external dissemination control and handling markings approved by ISOO or, with respect to the Intelligence Community by the Director of National Intelligence for intelligence and intelligence-related information, may be used by agencies to control and handle the dissemination of classified information pursuant to agency regulations and to policy directives and guidelines issued under section 5.4(d)(2) and section 6.2(b) of the Order. Such approved markings shall be uniform and binding on all agencies and must be available in a central registry.
(3) If used, the dissemination control and handling markings will appear at the top and bottom of each page after the level of classification.

(k) Portion marking waivers.

(1) An agency head or senior agency official may request a waiver from the portion marking requirement for a specific category of information. Such a request shall be submitted to the Director of ISOO and should include the reasons that the benefits of portion marking are outweighed by other factors. The request must also demonstrate that the requested waiver will not create impediments to information sharing. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.
(2) Any approved portion marking waiver will be temporary with specific expiration dates.
(3) Requests for portion marking waivers from elements of the Intelligence Community (to include pertinent elements of the Department of Defense) should include a statement of support from the Director of National Intelligence or his or her designee. Requests for portion marking waivers from elements of the Department of Defense (to include pertinent elements of the Intelligence Community) should include a statement of support from the Secretary of Defense or his or her designee. Requests for portion marking waivers from elements of the Department of Homeland Security should include a statement of support from the Secretary of Homeland Security or his or her designee.
(4) A document not portion marked, based on an ISOO-approved waiver, must contain a warning statement that it may not be used as a source for derivative classification.

(5) If a classified document that is not portion marked, based on an ISOO-approved waiver, is transmitted outside the originating organization, the document must be portion marked unless otherwise explicitly provided in the waiver approval.

(i) Marking information that has been reclassified.

Specific information may only be reclassified if all the conditions of section 1.7(d) of the Order and its implementing directives have been met.

(1) When taking this action, an original classification authority must include the following markings on the information:

(i) The level of classification;

(ii) The identity, by name and position, or by personal identifier of the original classification authority;

(iii) Declassification instructions;

(iv) A concise reason for classification, including reference to the applicable classification category from section 1.4 of the Order; and

(v) The date the reclassification action was taken.

(2) The original classification authority shall notify all known authorized holders of this action.

(m) Marking of electronic storage media.

Classified computer media such as USB sticks, hard drives, CD ROMs, and diskettes shall be marked to indicate the highest overall classification of the information contained within the media.


(a) General.

A uniform security classification system requires that standard markings be applied to declassified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of declassified information shall not deviate from the following prescribed formats. If declassification markings cannot be affixed to specific information or materials, the originator shall provide holders or recipients of the information with written instructions for marking the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the declassified status of the information and who authorized the declassification.

(b) The following markings shall be applied to records, or copies of records, regardless of media:

(1) The word, “Declassified;”
(2) The identity of the declassification authority, by name and position, or by personal identifier, or the title and date of the declassification guide. If the identity of the declassification authority must be protected, a personal identifier may be used or the information may be retained in agency files.

(3) The date of declassification; and

(4) The overall classification markings that appear on the cover page or first page shall be lined with an “X” or straight line. An example might appear as:

SECRET
Declassified by David Smith, Chief, Division 5, August 17, 2008


(a) Marking information exempted from automatic declassification at 25 years.

(1) When the Panel has approved an agency proposal to exempt permanently valuable information from automatic declassification at 25 years, the “Declassify On” line shall be revised to include the symbol “25X” plus the number(s) that corresponds to the category(ies) in section 3.3(b) of the Order. Except for when the exemption pertains to information that should clearly and demonstrably be expected to reveal the identity of a confidential human source, or a human intelligence source, or key design concepts of weapons of mass destruction, the revised “Declassify On” line shall also include the new date for declassification as approved by the Panel, not to exceed 50 years from the date of origin of the record. Records that contain information, the release of which should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, are exempt from automatic declassification at 50 years.

(2) The pertinent exemptions, using the language of section 3.3(b) of the Order, are:
25X1: reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.

25X2: reveal information that would assist in the development, production, or use of weapons of mass destruction;

25X3: reveal information that would impair U.S. cryptologic systems or activities;

25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

25X5: reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

25X6: reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

25X7: reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

25X8: reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

25X9: violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(3) The pertinent portion of the marking would appear as:

Declassify On: 25X4, 20501001

(4) Documents should not be marked with a “25X” marking until the agency has been informed that the Panel concurs with the proposed exemption.

(5) Agencies need not apply a “25X” marking to individual documents contained in a file series exempted from automatic declassification under section 3.3(c) of the Order until the individual document is removed from the file and may only apply such a marking as approved by the Panel under section 3.3(j) of the Order.

(6) Information containing foreign government information will be marked with a date in the “Declassify On” line that is no more than 25 years from the date of the document unless the originating agency has applied for and received Panel
approval to exempt foreign government information from declassification at 25 years. Upon receipt of Panel approval, the agency may use either the 25X6 or 25X9 exemption markings, as appropriate, in the “Declassify On” followed by a date that has also been approved by the Panel. An example might appear as: 25X6, 20600129, or 25X9, 20600627. The marking “subject to treaty or international agreement” is not to be used at any time.

(b) Marking information exempted from automatic declassification at 50 years.

Records exempted from automatic declassification at 50 years shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within five years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(1) When the information clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence source, the marking shall be “50X1-HUM.”

(2) When the information clearly and demonstrably could reveal key design concepts of weapons of mass destruction, the marking shall be “50X2-WMD.”

(3) In extraordinary cases in which the Panel has approved an exemption from declassification at 50 years under section 3.3(h) of the Order, the same procedures as those under § 2001.26(a) will be followed with the exception that the number “50” will be used in place of the “25.”

(4) Requests for exemption from automatic declassification at 50 years from elements of the Intelligence Community (to include pertinent elements of the Department of Defense) should include a statement of support from the Director of National Intelligence or his or her designee. Requests for automatic declassification exemptions from elements of the Department of Defense (to include pertinent elements of the Intelligence community) should include a statement of support from the Secretary of Defense or his or her designee. Requests for automatic declassification exemptions from elements of the Department of Homeland Security should include a statement of support from the Secretary of the Department of Homeland Security or his or her designee.

(c) Marking information exempted from automatic declassification at 75 years.

Records exempted from automatic declassification at 75 years shall be automatically declassified on December 31 of the year that has been formally approved by the Panel.

(1) Information approved by the Panel as exempt from automatic declassification at 75 years shall be marked “75X” with the appropriate automatic declassification exemption category number followed by the approved declassification date or event.

(2) Requests for exemption from automatic declassification at 75 years from elements of the Intelligence Community (to include pertinent elements of the Department of Defense) should include a statement of support from the Director.
of National Intelligence or his or her designee. Requests for automatic declassification exemptions from elements of the Department of Defense (to include pertinent elements of the Intelligence community) should include a statement of support from the Secretary of Defense or his or her designee.
SUBPART D—Declassification

(a) General.

All departments and agencies that have original classification authority or previously had original classification authority, or maintain records determined to be permanently valuable that contain classified national security information, shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in managing automatic declassification of accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist.

(b) Presidential papers, materials, and records.

The Archivist shall establish procedures for the declassification of presidential, vice-presidential, or White House materials transferred to the legal custody of NARA or maintained in the presidential libraries.

(c) Classified information in the custody of contractors, licensees, certificate holders, or grantees.

Pursuant to the provisions of the National Industrial Security Program, agencies must provide security classification/declassification guidance to such entities or individuals who possess classified information. Agencies must also determine if classified Federal records are held by such entities or individuals, and if so, whether they are permanent records of historical value and thus subject to section 3.3 of the Order. Until such a determination has been made by an appropriate agency official, such records shall not be subject to automatic declassification, or destroyed, and shall be safeguarded in accordance with the most recent security classification/declassification guidance provided by the agency.

(d) Transferred information.

In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage, the receiving agency shall be deemed to be the originating agency.

(e) Unofficially transferred information.

In the case of classified information that is not officially transferred as described in paragraph (d) of this section but that originated in an agency that has ceased to exist and for which there is no successor agency, the agency in possession shall serve as the originating agency and shall be responsible for actions for those
records in accordance with section 3.3 of the Order and in consultation with the Director of the National Declassification Center (NDC).

(f) Processing records originated by another agency.

When an agency uncovers classified records originated by another agency that appear to meet the criteria for referral according to section 3.3(d) of the Order, the finding agency shall identify those records for referral to the originating agency as described in § 2001.34.

(g) Unscheduled records.

Classified information in records that have not been scheduled for disposal or retention by NARA is not subject to section 3.3 of the Order. Classified information in records that become scheduled as permanently valuable when that information is already more than 20 years old shall be subject to the automatic declassification provisions of section 3.3 of the Order five years from the date the records are scheduled. Classified information in records that become scheduled as permanently valuable when that information is less than 20 years old shall be subject to the automatic declassification provisions of section 3.3 of the Order at 25 years.

(h) Temporary records and non-record materials.

Classified information contained in records determined not to be permanently valuable or non-record materials shall be processed in accordance with section 3.6(c) of the Order.

(i) Foreign government information.

The declassifying agency is the agency that initially received or classified the information. When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification. The declassifying agency shall also determine if another exemption under section 3.3(b) of the Order, such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government prior to declassification.

(j) Assistance to the Archivist of the United States.

Agencies shall consult with the Director of the NDC established in section 3.7 of the Order concerning their automatic declassification programs. At the request of the Archivist, agencies shall cooperate with the Director of the NDC in developing
priorities for the declassification of records to ensure that declassification is accomplished efficiently and in a timely manner. Agencies shall consult with NARA and the Director of the NDC before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that NARA receives accurate and sufficient information about agency declassification actions, including metadata and other processing information, when records are accessioned by NARA. This data shall include certification by the agency that the records have been reviewed in accordance with Public Law 105-261, section 3161 governing Restricted Data and Formerly Restricted Data.

(k) Use of approved declassification guides.

Approved declassification guides are the sole basis for the exemption from automatic declassification of specific information as provided in section 3.3(b) of the Order and the sole basis for the continued classification of information under section 3.3(h) of the Order. These guides must be prepared in accordance with section 3.3(j) of the Order and include additional pertinent detail relating to the exemptions described in sections 3.3(b) and 3.3(h) of the Order, and follow the format required of declassification guides as described in § 2001.32. During a review under section 3.3 of the Order, it is expected that agencies will use these guides to identify specific information for exemption from automatic declassification. It is further expected that the guides or detailed declassification guidance will be made available to the NDC under section 3.7(b) of the Order and to appropriately cleared individuals of other agencies to support equity recognition.

(l) Automatic declassification date.

No later than December 31 of the year that is 25 years from the date of origin, classified records determined to be permanently valuable shall be automatically declassified unless automatic declassification has been delayed for any reason as provided in § 2001.30(n) and sections 3.3(b) and (c) of the Order. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(m) Exemption from Automatic Declassification at 25, 50, or 75 years.

Agencies may propose to exempt from automatic declassification specific information, either by reference to information in specific records, in specific file series of records, or in the form of a declassification guide, in accordance with section 3.3(j) of the Order. Agencies may propose to exempt information within five years of, but not later than one year before the information is subject to automatic declassification. The agency head or senior agency official, within the specified timeframe, shall notify the Director of ISOO, serving as the Executive Secretary of the Panel, of the specific information being proposed for exemption from automatic declassification.
(n) Delays in the onset of automatic declassification

(1) Media that make a review for possible declassification exemptions more difficult or costly.
An agency head or senior agency official shall consult with the Director of the NDC before delaying automatic declassification for up to five years for classified information contained in media that make a review for possible declassification more difficult or costly. When determined by NARA or jointly determined by NARA and another agency, the following may be delayed due to the increased difficulty and cost of conducting declassification processing:
(i) Records requiring extraordinary preservation or conservation treatment, to include reformatting, to preclude damage to the records by declassification processing;
(ii) Records which pose a potential menace to health, life, or property due to contamination by a hazardous substance; and
(iii) Electronic media if the media is subject to issues of software or hardware obsolescence or degraded data.

(2) Referred records.
Records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies and could reasonably be expected to fall under one or more of the exemption categories of section 3.3(b) of the Order shall be identified prior to the onset of automatic declassification for later referral to those agencies. Declassification reviewers shall be trained periodically on other agency equities to aid in the proper identification of other agency equities eligible for referral.
(i) Information properly identified as a referral to another agency contained in records accessioned by NARA or in the custody of the presidential libraries shall be subject to automatic declassification only after the referral has been made available by NARA for agency review in accordance with § 2001.34, provided the information has not otherwise been properly exempted by an equity holding agency under section 3.3 of the Order.
(ii) Information properly identified as a referral to another agency contained in records maintained in the physical, but not legal, custody of NARA shall be subject to automatic declassification after accessioning and in accordance with § 2001.34, provided the information has not otherwise been properly exempted by an equity holding agency under section 3.3 of the Order.

(3) Newly discovered records.
An agency head or senior agency official must consult with the Director of ISOO on any decision to delay automatic declassification of newly discovered records no later than 90 days, from the discovery of the records. The notification shall identify the records, their volume, the anticipated date for declassification, and the circumstances of the discovery. An agency may be granted up to three years from the date of discovery to make a declassification, exemption, or referral determination. If referrals to other agencies are properly identified, they will be handled in accordance with subparagraphs 2(i) and 2(ii) above.

Page 1137
(4) **Integral file blocks.**
Classified records within an integral file block that are otherwise subject to automatic declassification under section 3.3 of the Order shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block. For purposes of automatic declassification, integral file blocks shall contain only records dated within ten years of the oldest record in the file block. Integral file blocks applied prior to December 29, 2009, that cover more than ten years remain in effect until December 31, 2012, unless an agency requests an extension from the Director of ISOO on a case-by-case basis prior to December 31, 2011, which is subsequently approved.

(5) **File series exemptions.**
Agencies seeking to delay the automatic declassification of a specific series of records as defined in section 6.1(r) of the Order because it almost invariably contains information that falls within one or more of the exemption categories under section 3.3(b) must submit their request in accordance with section 3.3(c) of the Order to the Director of ISOO, serving as Executive Secretary of the Panel, at least one year prior to the onset of automatic declassification. Once approved by the Panel, the records in the file series exemption remain subject to section 3.5 of the Order. This delay applies only to records within the specific file series. Copies of records within the specific file series or records of a similar topic to the specific file series located elsewhere may be exempted in accordance with exemptions approved by the Panel.

(o) **Redaction standard.**

Agencies are encouraged but are not required to redact documents that contain information that is exempt from automatic declassification under section 3.3 of the Order, especially if the information that must remain classified comprises a relatively small portion of the document. Any such redactions shall be performed in accordance with policies and procedures established in accordance with § 2001.45(d).

(p) **Restricted Data and Formerly Restricted Data.**

(1) Restricted Data and Formerly Restricted Data are excluded from the automatic declassification requirements in section 3.3 of the Order because they are classified under the Atomic Energy Act of 1954, as amended. Restricted Data concerns:
(i) The design, manufacture, or utilization of atomic weapons;
(ii) The production of special nuclear material, e.g., enriched uranium or plutonium; or
(iii) The use of special nuclear material in the production of energy.

(2) Formerly Restricted Data is information that is still classified under the Atomic Energy Act of 1954, as amended, but which has been removed from the
Restricted Data category because it is related primarily to the military utilization of atomic weapons.

(3) Any document marked as containing Restricted Data or Formerly Restricted Data or identified as potentially containing unmarked Restricted Data or Formerly Restricted Data shall be referred to the Department of Energy in accordance with § 2001.34(b)(8).

(4) Automatic declassification of documents containing Restricted Data or Formerly Restricted Data is prohibited. Documents marked as containing Restricted Data or Formerly Restricted Data are excluded from the automatic declassification provisions of the Order until the Restricted Data or Formerly Restricted Data designation is properly removed by the Department of Energy. When the Department of Energy determines that a Restricted Data or Formerly Restricted Data designation may be removed, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification provisions of the Order and this Directive.

(5) Any document containing information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, shall be referred to the Department of Energy.

(6) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out the provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, information concerning foreign nuclear programs (e.g., intelligence assessments or reports, foreign nuclear program information provided to the U.S. Government) shall be declassified when comparable information concerning the United States nuclear program is declassified. When the Secretary of Energy determines that information concerning foreign nuclear programs may be declassified, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification provisions of the Order and this Directive.


(a) General.

Agencies shall establish systematic review programs for those records containing information exempted from automatic declassification. This includes individual records as well as file series of records. Agencies shall prioritize their review of such records in accordance with priorities established by the NDC.


(a) Preparation of declassification guides.
Beginning one year after the effective date of this directive, declassification guides must be submitted to the Director of ISOO, serving as the Executive Secretary of the Panel, at least one year prior to the onset of automatic declassification for approval by the Panel. Currently approved guides remain in effect until a new guide is approved, to the extent they are otherwise applied consistent with section 3.3(b) of the Order. The information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions must be based upon specific content and not type of document. Exemptions for general categories of information are not acceptable. Agencies must prepare guides that clearly delineate between the exemptions proposed under sections 3.3(b), 3.3(h)(1) and (2), and 3.3(h)(3).

(b) General content of declassification guides.

Declassification guides must be specific and detailed as to the information requiring continued classification and clearly and demonstrably explain the reasons for continued classification. Declassification guides shall:
(1) Be submitted by the agency head or the designated senior agency official;
(2) Provide the date of issuance or last review;
(3) State precisely the information that the agency proposes to exempt from automatic declassification and to specifically declassify;
(4) Identify any related files series that have been exempted from automatic declassification pursuant to section 3.3(c) of the Order; and
(5) To the extent a guide is used in conjunction with the automatic declassification provisions in section 3.3 of the Order, state precisely the elements of information to be exempted from declassification to include:
   (i) The appropriate exemption category listed in section 3.3(b), and, if appropriate, section 3.3(h) of the Order; and
   (ii) A date or event for declassification that is in accordance with section 3.3(b) or section 3.3(h).

(c) Internal review and update.

Agency declassification guides shall be reviewed and updated as circumstances require, but at least once every five years. Each agency shall maintain a list of its declassification guides in use.

(d) Dissemination of guides.

(1) Declassification guides shall be disseminated within the agency to be used by all personnel with declassification review responsibilities.
(2) Declassification guides or detailed declassification guidance shall be submitted to the Director of the NDC in accordance with section 3.7(b)(3) of the Order.

(a) U.S. originated information

(1) Regulations.
Each agency shall publish, and update as needed or required, in the Federal Register regulations concerning the handling of mandatory declassification review requests, to include the identity of the person(s) or office(s) to which requests should be addressed.

(2) Processing
—(i) Requests for classified records in the custody of the originating agency.
A valid mandatory declassification review request must be of sufficient specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Requests for broad types of information, entire file series of records, or similar non-specific requests may be denied by agencies for processing under this section. In responding to mandatory declassification review requests, agencies shall make a final determination within one year from the date of receipt. When information cannot be declassified in its entirety, agencies shall make reasonable efforts to release, consistent with other applicable laws, those declassified portions of the requested information that constitute a coherent segment. Upon denial, in whole or in part, of an initial request, the agency shall also notify the requestor of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial. Agencies receiving mandatory review requests are expected to conduct a line-by-line review of the record(s) for public access and are expected to release the information to the requestor, unless that information is prohibited from release under the provisions of a statutory authority, such as, but not limited to, the Freedom of Information Act, (5 U.S.C. 552), as amended, the Presidential Records Act of 1978 (44 U.S.C. 2201-2207), or the National Security Act of 1947 (Pub. L. 235, 61 Stat. 496, 50 U.S.C. Chapter 15).

(ii) Requests for classified records in the custody of an agency other than the originating agency.
When an agency receives a mandatory declassification review request for records in its possession that were originated by another agency, it shall refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, the custodial agency shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, the originating agency shall promptly process the request for declassification and release in accordance with this section. The originating agency shall communicate its declassification determination to the referring agency. The referring agency is responsible for collecting all agency review results and informing the requestor of any final decision regarding the declassification of the requested information unless a prior arrangement has been made with the originating agency.

(iii) Appeals of denials of mandatory declassification review requests.
The agency appellate authority shall normally make a determination within 60 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requestor in writing of the final determination and of the reasons for any denial. The appellate authority must inform the requestor of his or her final appeal rights to the Panel.

(iv) Appeals to the Interagency Security Classification Appeals Panel.

In accordance with section 5.3(c) of the Order, the Panel shall publish in the Federal Register the rules and procedures for bringing mandatory declassification appeals before it.

(v) Records subject to mandatory declassification review.

Records containing information exempted from automatic declassification in accordance with section 3.3(c) of the Order or with § 2001.30(n)(1) are still subject to the mandatory declassification review provisions of section 3.5 of the Order.

(b) Foreign government information.

Except as provided in this paragraph, agencies shall process mandatory declassification review requests for classified records containing foreign government information in accordance with this section. The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government(s) prior to declassification.

(c) Cryptologic information.

Mandatory declassification review requests for cryptologic information shall be processed in accordance with special procedures issued by the Secretary of Defense and, when cryptologic information pertains to intelligence activities, the Director of National Intelligence.

(d) Intelligence information.

Mandatory declassification review requests for information pertaining to intelligence sources, methods, and activities shall be processed in accordance with special procedures issued by the Director of National Intelligence.

(e) Fees.
In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with 31 U.S.C. 9701 or relevant fee provisions in other applicable statutes.

(f) Requests filed under mandatory declassification review and the Freedom of Information Act.

When a requester submits a request both under mandatory declassification review and the Freedom of Information Act (FOIA), the agency shall require the requestor to select one process or the other. If the requestor fails to select one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory declassification review.

(g) FOIA and Privacy Act requests.

Agency heads shall process requests for declassification that are submitted under the provisions of the FOIA, as amended, or the Privacy Act of 1974 (5 U.S.C. 552a), as amended, in accordance with the provisions of those Acts.

(h) Redaction standard.

Agencies shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction. The specific reason for the redaction, as provided for in section 1.4 or 3.3(b) of the Order, as applicable, must be included for each redaction. Information that is redacted due to a statutory authority must be clearly marked with the specific authority that authorizes the redaction. Any such redactions shall be performed in accordance with policies and procedures established in accordance with § 2001.45(d).

(i) Limitations on requests.

Requests for mandatory declassification review made to an element of the Intelligence Community by anyone other than a citizen of the United States or an alien lawfully admitted for permanent residence, may be denied by the receiving Intelligence Community element. Documents required to be submitted for pre-publication review or other administrative process pursuant to an approved nondisclosure agreement are not subject to mandatory declassification review.


(a) General.

Referrals are required under sections 3.3(d)(3) and 3.6(b) of the Order in order to ensure the timely, efficient, and effective processing of reviews and requests and in order to protect classified information from inadvertent disclosure.

(b) Automatic declassification.
The referral process for records subject to automatic declassification entails identification of records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies. Those records that could reasonably be expected to fall under one or more of the exemptions in section 3.3(b) of the Order are eligible for referral. The referral process also entails formal notification to those agencies, making the records available for review by those agencies, and recording final agency determinations.

(1) In accordance with section 3.3(d)(3) of the Order, the identification of records eligible for referral is the responsibility of the primary reviewing agency and shall be completed prior to the date of automatic declassification established by section 3.3(a) of the Order.

(2) Except as otherwise determined by the Director of the NDC, primary reviewing agencies shall utilize the Standard Form 715, Government Declassification Review Tab, to tab and identify any Federal record requiring referral and record the referral in a manner that provides the referral information in an NDC database system.

(3) Notification of referral of records accessioned into NARA or in the custody of the presidential libraries, and making the records available for review, is the responsibility of NARA and shall be accomplished through the NDC.

(4) Within 180 days of the effective date of this provision, the NDC shall develop and provide the affected agencies with a comprehensive and prioritized schedule for the resolution of referrals contained in accessioned Federal records and Presidential records. The schedule shall be developed in consultation with the affected agencies, consider the public interest in the records, and be in accordance with the authorized delays to automatic declassification set forth in section 3.3(d) of the Order. The initial schedule shall cover the balance of the first effective fiscal year and four subsequent fiscal years. Thereafter, the schedule shall cover five fiscal years. The NDC shall consult with the affected agencies and update and provide such schedules annually.

(5) The NDC shall provide formal notification of the availability of a referral to the receiving agency and records will be subject to automatic declassification in accordance with the schedule promulgated by the NDC in paragraph (b)(4) of this section, unless the information has been properly exempted by an equity holding agency under section 3.3 of the Order.

(6) Records in the physical but not legal custody of NARA shall be subject to automatic declassification after accessioning and in accordance with paragraphs (b)(3) and (b)(5) of this section.

(7) Agencies that establish a centralized facility as described in section 3.7(e) may make direct referrals provided such activities fall within the priorities and schedule established by the NDC and the activity is otherwise coordinated with the NDC. In such cases, the centralized facility is responsible for providing formal notification of a referral to receiving agencies and for making the records available for review or direct formal referral to agencies by providing a copy of the records unless another mechanism is identified in coordination with the NDC. As established in section 3.3(d)(3)(B), referrals to agencies from a
centralized agency records facility as described in section 3.7(e) of the Order will be automatically declassified up to three years after the formal notification has been made, if the receiving agency fails to provide a final determination.

(8) Records marked as containing Restricted Data or Formerly Restricted Data or identified as potentially containing unmarked Restricted Data or Formerly Restricted Data shall be referred to the Department of Energy through the NDC. If the Department of Energy confirms that the document contains Restricted Data or Formerly Restricted Data, it shall then be excluded from the automatic declassification provisions of the Order until the Restricted Data or Formerly Restricted Data designation is properly removed.

(i) When the Department of Energy provides notification that a Restricted Data or Formerly Restricted Data designation is not appropriate or when it is properly removed, the record shall be processed for automatic declassification through the NDC.

(ii) In all cases, should the record be the subject of an access demand made pursuant to the Order or provision of law, the information classified pursuant to Executive order (rather than the Atomic Energy Act, as amended) must stand on its own merits.

(9) The NDC, as well as any centralized agency facility established under section 3.7(e) of the Order, shall track and document referral actions and decisions in a manner that facilitates archival processing for public access. Central agency facilities must work with the NDC to ensure documentation meets NDC requirements, and transfer all documentation on pending referral actions and referral decisions to the NDC when transferring the records to NARA.

(10) In all cases, receiving agencies shall acknowledge receipt of formal referral notifications in a timely manner. If a disagreement arises concerning referral notifications, the Director of ISOO will determine the automatic declassification date and notify the senior agency official, as well as the NDC or the primary reviewing agency.

(11) Remote Archives Capture (RAC).

Presidential records or materials scanned in the RAC process shall be prioritized and scheduled for review by the NDC. The initial notification shall be made to the agency with primary equity, which shall have up to one year to act on its information and to identify all other equities eligible for referral. All such additional referrals in an individual record shall be made at the same time, and once notified by the NDC of an eligible referral, such receiving agencies shall have up to one year to review the records before the onset of automatic declassification.

(c) Agencies eligible to receive referrals.

The Director of ISOO will publish annually a list of those agencies eligible to receive referrals for each calendar year.

(d) Systematic declassification review.
The identification of equities shall be accomplished in accordance with paragraph (b) of this section. Priorities for review will be established by the NDC.

(e) Identification of interests other than national security.

Referrals under sections 3.3(d)(3) and 3.6(b) of the Order shall be assumed to be intended for later public release unless withholding is otherwise authorized and warranted under applicable law. If a receiving agency proposes to withhold any such information, it must notify the referring agency at the time they otherwise respond to the referral. Such notification shall identify the specific information at issue and the pertinent law.

32 CFR Section 2001.35: Discretionary declassification.
(a) In accordance with section 3.1(d) of the Order, agencies may declassify information when the public interest in disclosure outweighs the need for continued classification.
(b) Agencies may also establish a discretionary declassification program that is separate from their automatic, systematic, and mandatory review programs.

32 CFR Section 2001.36: Classified information in the custody of private organizations or individuals.

(a) Authorized holders.

Agencies may allow for the holding of classified information by a private organization or individual provided that all access and safeguarding requirements of the Order have been met. Agencies must provide declassification assistance to such organizations or individuals.

(b) Others.

Anyone who becomes aware of organizations or individuals who possess potentially classified national security information outside of government control must contact the Director of ISOO for guidance and assistance. The Director of ISOO, in consultation with other agencies, as appropriate, will ensure that the safeguarding and declassification requirements of the Order are met.

32 CFR Section 2001.37: Assistance to the Department of State.
Heads of agencies shall assist the Department of State in its preparation of the Foreign Relations of the United States (FRUS) series by facilitating access to appropriate classified materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS. If an agency fails to provide a final declassification review determination regarding a Department of State referral within 120 days of the date of the referral, or if applicable, within 120 days of the date of a High Level Panel decision, the Department of State, consistent with 22 U.S.C. 4353 and any implementing agency procedures, may seek the assistance of the Panel.
SUBPART E—Safeguarding


(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.

(b) Except for foreign government information, agency heads or their designee(s) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director of ISOO. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value, and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasure benefits versus cost.

(c) North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instruction (USSAN) 1-07. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at § 2001.54 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) Need-to-know determinations.

(1) Agency heads, through their designees, shall identify organizational missions and personnel requiring access to classified information to perform or assist in authorized governmental functions. These mission and personnel requirements are determined by the functions of an agency or the roles and responsibilities of personnel in the course of their official duties. Personnel determinations shall be consistent with section 4.1(a) of the Order.

(2) In instances where the provisions of section 4.1(a) of the Order are met, but there is a countervailing need to restrict the information, disagreements that cannot be resolved shall be referred by agency heads or designees to either the Director of ISOO or, with respect to the Intelligence Community, the Director of National Intelligence, as appropriate. Disagreements concerning information protected under section 4.3 of the Order shall instead be referred to the appropriate official named in section 4.3 of the Order.


Authorized persons who have access to classified information are responsible for:
(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;
(b) Meeting safeguarding requirements prescribed by the agency head; and
(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.


(a) Storage.

The Administrator of the General Services Administration (GSA) shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications, qualified product lists or databases, and supply schedules for security equipment designed to provide secure storage for classified information. Whenever new secure storage equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of the GSA, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

(b) Destruction.

Effective January 1, 2011, only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy classified information using any method covered by an EPL. However, equipment approved for use prior to January 1, 2011, and not found on an EPL, may be utilized for the destruction of classified information until December 31, 2016. Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be utilized for the destruction of classified information up to six years from the date of its removal from an EPL. In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for the destruction in accordance with this section. The Administrator of the GSA shall, to the maximum extent possible, coordinate supply schedules and otherwise seek to make equipment on an EPL available through the Federal Supply System.


(a) General.

Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government-controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities
under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) Requirements for physical protection

(1) Top Secret.
Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53. In addition, supplemental controls are required as follows:
(i) For GSA-approved containers, one of the following supplemental controls:
(A) Inspection of the container every two hours by an employee cleared at least to the Secret level;
(B) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of Intrusion Detection Equipment (IDE): All IDE must be in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head; or
(C) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF-L-2740.
(ii) For open storage areas covered by Security-In-Depth, an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.
(iii) For open storage areas not covered by Security-In-Depth, personnel responding to the alarm shall arrive within five minutes of the alarm annunciation.

(2) Secret.
Secret information shall be stored in the same manner as Top Secret information or, until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock. Security-In-Depth is required in areas in which a non-GSA-approved container or open storage area is located. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required:
(i) Inspection of the container or open storage area every four hours by an employee cleared at least to the Secret level; or
(ii) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

(3) Confidential.
Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.
(c) Combinations.

Use and maintenance of dial-type locks and other changeable combination locks.

(1) Equipment in service.
Combinations to dial-type locks shall be changed only by persons authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:
(i) Whenever such equipment is placed into use;
(ii) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or
(iii) Whenever a combination has been subject to possible unauthorized disclosure.

(2) Equipment out of service.
When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the combination lock should be reset to a standard combination of 50-25-50 for built-in combination locks or 10-20-30 for combination padlocks.

(d) Key operated locks.
When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be included in implementing regulations required under section 5.4(d)(2) of the Order.

(e) Repairs.
The neutralization and repair of GSA-approved security containers and vault doors will be in accordance with FED STD 809.

32 CFR Section 2001.44: Reciprocity of use and inspection of facilities.
(a) Once a facility is authorized, approved, certified, or accredited for classified use, then all agencies desiring to conduct classified work in the designated space(s) at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades provided that no waiver, exception, or deviation has been issued or approved. In the event that a waiver exception, or deviation was granted in the original accreditation of the designated space(s), an agency seeking to utilize the designated facility space may require that a risk mitigation strategy be implemented or agreed upon prior to using the space(s).
(b) Subsequent security inspections or reviews for authorization, approval, certification, or accreditation purposes shall normally be conducted no more
frequently than annually unless otherwise required due to a change in the designated facility space(s) or due to a change in the use or ownership of the facility space(s). This does not imply a formal one-year inspection or review requirement or establish any other formal period for inspections or review.


(a) General.

Agency heads shall establish a system of control measures which assure that access to classified information is provided to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(1) Combinations.
Combinations to locks used to secure vaults, open storage areas, and security containers that are approved for the safeguarding of classified information shall be protected in the same manner as the highest level of classified information that the vault, open storage area, or security container is used to protect.

(2) Computer and information system passwords.
Passwords shall be protected in the same manner as the highest level of classified information that the computer or system is certified and accredited to process. Passwords shall be changed on a frequency determined to be sufficient to meet the level of risk assessed by the agency.

(b) Reproduction.

Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken:
(1) Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;
(2) Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;
(3) Copies of classified information shall be subject to the same controls as the original information; and
(4) The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged.

(c) Forms.
The use of standard forms prescribed in subpart H of this part is mandatory for all agencies that create and/or handle national security information.

(d) Redaction

(1) Policies and procedures.  
Classified information may be subject to loss, compromise, or unauthorized disclosure if it is not correctly redacted. Agencies shall establish policies and procedures for the redaction of classified information from documents intended for release. Such policies and procedures require the approval of the agency head and shall be sufficiently detailed to ensure that redaction is performed consistently and reliably, using only approved redaction methods that permanently remove the classified information from copies of the documents intended for release. Agencies shall ensure that personnel who perform redaction fully understand the policies, procedures, and methods and are aware of the vulnerabilities surrounding the process.

(2) Technical guidance for redaction.  
Technical guidance concerning appropriate methods, equipment, and standards for the redaction of classified electronic and optical media shall be issued by NSA.


(a) General.

Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Directive.

(b) Dispatch.

Agency heads shall establish procedures which ensure that:

(1) All classified information physically transmitted outside facilities shall be enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. The outer enclosure shall be the same except that no markings to indicate that the contents are classified shall be visible. Intended recipients shall be identified by name only as part of an attention line. The following exceptions apply:

(i) If the classified information is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;
(ii) If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;
(iii) If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;
(iv) Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and
(v) When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.
(2) Couriers and authorized persons designated to hand-carry classified information shall ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a combination padlock meeting Federal Specification FF-P-110, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(c) Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory.

(1) Top Secret.
Top Secret information shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or any other cleared or uncleared commercial carrier.

(2) Secret.
Secret information shall be transmitted by:
(i) Any of the methods established for Top Secret; U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, as long as the Waiver of Signature block on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited; and
(ii) Agency heads may, when a requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the GSA contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations (39 CFR. Chapter I) are met. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with government inquiries in the event of a
loss, theft, or possible unauthorized disclosure of classified information. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information shall not be transmitted in this manner.

(3) Confidential.
Confidential information shall be transmitted by any of the methods established for Secret information or U.S. Postal Service Certified Mail. In addition, when the recipient is a U.S. Government facility, the Confidential information may be transmitted via U.S. First Class Mail. However, Confidential information shall not be transmitted to government contractor facilities via first class mail. When first class mail is used, the envelope or outer wrapper shall be marked to indicate that the information is not to be forwarded, but is to be returned to sender. The use of streetside mail collection boxes is prohibited.

(d) Transmission methods to a U.S. Government facility located outside the U.S.

The transmission of classified information to a U.S. Government facility located outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, shall be by methods specified above for Top Secret information or by the Department of State Courier Service. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

(e) Transmission of U.S. classified information to foreign governments.

Such transmission shall take place between designated government representatives using the government-to-government transmission methods described in paragraph (d) of this section or through channels agreed to by the National Security Authorities of the two governments. When classified information is transferred to a foreign government or its representative a signed receipt is required.

(f) Receipt of classified information.

Agency heads shall establish procedures which ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. As noted in paragraph (e) of this section, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative is required.
Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. Agencies shall comply with the destruction equipment standard stated in § 2001.42(b) of this Directive.

32 CFR Section 2001.48: Loss, possible compromise or unauthorized disclosure.

(a) General.

Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) Cases involving information originated by a foreign government or another U.S. government agency.

Whenever a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government agency, or another U.S. government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

(c) Inquiry/investigation and corrective actions.

Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) Reports to ISOO.

In accordance with section 5.5(e)(2) of the Order, agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of the Order that:
(1) Is reported to oversight committees in the Legislative branch;
(2) May attract significant public attention;
(3) Involves large amounts of classified information; or
(4) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(e) Department of Justice and legal counsel coordination.

Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with:

(1) The Department of Justice, and
(2) The legal counsel of the agency where the individual responsible is assigned or employed.

32 CFR Section 2001.49: Special access programs.

(a) General.

The safeguarding requirements of this Directive may be enhanced for information in special access programs (SAP), established under the provisions of section 4.3 of the Order by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

(b) Significant interagency support requirements.

Agency heads must ensure that a Memorandum of Agreement/Understanding is established for each SAP that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

32 CFR Section 2001.50: Telecommunications automated information systems and network security.

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation.


Based upon the risk management factors referenced in § 2001.40 of this directive, agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures and TEMPEST necessary to detect or deter exploitation of classified information.
through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, TEMPEST Countermeasures for Facilities, and SPB Issuance 6-97, National Policy on Technical Surveillance Countermeasures.

(a) Agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations.
(b) In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:
(1) Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;
(2) Limit the number of individuals who receive it;
(3) Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in § 2001.46, or other means deemed necessary when time is of the essence;
(4) Provide instructions about what specific information is classified and how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances;
(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement;
(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:
(i) A description of the disclosed information;
(ii) To whom the information was disclosed;
(iii) How the information was disclosed and transmitted;
(iv) Reason for the emergency release;
(v) How the information is being safeguarded; and
(vi) A description of the briefings provided and a copy of the nondisclosure agreements signed.
(7) Information disclosed in emergency situations shall not be required to be declassified as a result of such disclosure or subsequent use by a recipient.

32 CFR Section 2001.53: Open storage areas.
This section describes the minimum construction standards for open storage areas.

(a) Construction.
The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.

(b) Doors.

Doors shall be constructed of wood, metal, or other solid material. Entrance doors shall be secured with a built-in GSA-approved three-position combination lock. When special circumstances exist, the agency head may authorize other locks on entrance doors for Secret and Confidential storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head.

(c) Vents, ducts, and miscellaneous openings.

All vents, ducts, and similar openings in excess of 96 square inches (and over 6 inches in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system.

(d) Windows.

(1) All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

(2) Windows within 18 feet of the ground will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area).

The requirements described below are additional baseline safeguarding standards that may be necessary for foreign government information, other than NATO information, that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation. NATO classified information shall be safeguarded in compliance with USSAN 1-07. To the extent practical, and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described in paragraphs (a) through (e) of this section may be modified if required or permitted by treaties or agreements,
or for other obligations, with the prior written consent of the National Security Authority of the originating government, hereafter “originating government.”

(a) Top Secret.

Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

(b) Secret.

Records shall be maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

(c) Confidential.

Records need not be maintained for foreign government Confidential information unless required by the originator.

(d) Restricted and other foreign government information provided in confidence.

In order to assure the protection of other foreign government information provided in confidence (e.g., foreign government “Restricted,” “Designated,” or unclassified provided in confidence), such information must be classified under the Order. The receiving agency, or a receiving U.S. contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, shall provide a degree of protection to the foreign government information at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the following requirements shall be met:

(1) Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents shall be marked, “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level).” The notation, “Modified Handling Authorized,” may be added to either the foreign or U.S. markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;
(2) Documents shall be provided only to persons in accordance with sections 4.1(a) and (h) of the Order;
(3) Individuals being given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;
(4) Documents shall be stored in such a manner so as to prevent unauthorized access;
(5) Documents shall be transmitted in a method approved for classified information, unless this method is waived by the originating government.

(e) Third-country transfers.

The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government or international organization of governments, or any element thereof, in accordance with statute, the Order, directives implementing the Order, direction of the President, or with the consent of the originating agency, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information. Markings used to implement this section shall be approved in accordance with § 2001.24(j). With respect to the Intelligence Community, the Director of National Intelligence may issue policy directives or guidelines pursuant to section 6.2(b) of the Order that modify such prior authorization.
SUBPART F—Self-Inspections

(a) Purpose.

This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include regular reviews of representative samples of the agency's original and derivative classification actions.

(b) Responsibility.

The senior agency official is responsible for directing and administering the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility. The program shall be structured to provide the senior agency official with information necessary to assess the effectiveness of the classified national security information program within individual agency activities and the agency as a whole, in order to enable the senior agency official to fulfill his or her responsibility to oversee the agency's program under section 5.4(d) of the Order.

(c) Approach.

The senior agency official shall determine the means and methods for the conduct of self-inspections.

(1) Self-inspections should evaluate the adherence to the principles and requirements of the Order and this directive and the effectiveness of agency programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

(2) Regular reviews of representative samples of the agency's original and derivative classification actions shall encompass all agency activities that generate classified information. They shall include a sample of varying types of classified information (in document and electronic format such as e-mail) to provide a representative sample of the activity's classification actions. The sample shall be proportionally sufficient to enable a credible assessment of the agency's classified product. Agency personnel who are assigned to conduct reviews of agencies' original and derivative classification actions shall be knowledgeable of the classification and marking requirements of the Order and this directive, and have access to pertinent security classification guides. In accordance with section 5.4(d)(4) of the Order, the senior agency official shall authorize appropriate agency officials to correct misclassification actions.

(3) Self-inspections should include a review of relevant security directives and instructions, as well as interviews with producers and users of classified information.

(d) Frequency.
Self-inspections shall be regular, ongoing, and conducted at least annually with the senior agency official setting the frequency on the basis of program needs and the degree of classification activity. Activities that generate significant amounts of classified information shall include a representative sample of their original and derivative classification actions.

(e) Coverage.

The senior agency official shall establish self-inspection coverage requirements based on program and policy needs. Agencies with special access programs shall evaluate those programs in accordance with sections 4.3(b)(2) and (4) of the Order, at least annually.

(f) Reporting.

Agencies shall document the findings of self-inspections internally.

(1) Internal.

The senior agency official shall set the format for documenting self-inspection findings. As part of corrective action for findings and other concerns of a systemic nature, refresher security education and training should address the underlying cause(s) of the issue.

(2) External.

The senior agency official shall report annually to the Director of ISOO on the agency's self-inspection program. This report shall include:

(i) A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized;
(ii) The assessment and a summary of the findings of the agency self-inspections in the following program areas: Original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight;
(iii) Specific information with regard to the findings of the annual review of the agency's original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies that were identified;
(iv) Actions that have been taken or are planned to correct identified deficiencies or misclassification actions, and to deter their reoccurrence; and
(v) Best practices that were identified during self-inspections.
SUBPART G—Security Education and Training

(a) Purpose.

This subpart sets standards for agency security education and training programs. Implementation of these standards should:
(1) Ensure that all executive branch employees who create, process, or handle classified information have a satisfactory knowledge and understanding of classification, safeguarding, and declassification policies and procedures;
(2) Increase uniformity in the conduct of agency security education and training programs; and
(3) Reduce instances of over-classification or improper classification, improper safeguarding, and inappropriate or inadequate declassification practices.

(b) Responsibility.

The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel, as necessary, to assist in carrying out this responsibility.

(c) Approach.

Security education and training should be tailored to meet the specific needs of the agency's security program and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, on-line presentations, and other media and methods. Each agency shall maintain records about the programs it has offered and employee participation in them.

(d) Frequency.

The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program, subject to the following requirements:
(1) Initial training shall be provided to every person who has met the standards for access to classified information in accordance with section 4.1 of the Order.
(2) Original classification authorities shall receive training in proper classification and declassification prior to originally classifying information and at least once each calendar year thereafter.
(3) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the Order prior to derivatively classifying information and at least once every two years.
(4) Each agency shall provide some form of refresher security education and training at least annually for all its personnel who handle or generate classified information.


(a) General.

Each department or agency shall establish and maintain a formal security education and training program which provides for initial training, refresher training, specialized training, and termination briefings. This subpart establishes fundamental security education and training standards for original classification authorities, derivative classifiers, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. Agency officials responsible for the security education and training programs should determine the specific training to be provided according to the agency’s program and policy needs.

(b) Initial training.

All cleared agency personnel shall receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. Such training must be provided in conjunction with the granting of a security clearance, and prior to accessing classified information.

(c) Training for original classification authorities.

Original classification authorities shall be provided detailed training on proper classification and declassification, with an emphasis on the avoidance of over-classification. At a minimum, the training shall cover classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(1) Personnel shall receive this training prior to originally classifying information.

(2) In addition to this initial training, original classification authorities shall receive training in proper classification and declassification at least once each calendar year.

(3) Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended until such training has taken place.

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.
(ii) Whenever such a waiver is granted, the individual shall receive the required training as soon as practicable.

(d) Training for persons who apply derivative classification markings.

Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the Order, emphasizing the avoidance of over-classification. At a minimum, the training shall cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(1) Personnel shall receive this training prior to derivatively classifying information.
(2) In addition to this preparatory training, derivative classifiers shall receive such training at least once every two years.
(3) Derivative classifiers who do not receive such mandatory training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received such training.

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.
(ii) Whenever such a waiver is granted, the individual shall receive the required training as soon as practicable.

(e) Other specialized security education and training.

Classification management officers, security managers, security specialists, declassification authorities, and all other personnel whose duties significantly involve the creation or handling of classified information shall receive more detailed or additional training no later than six months after assumption of duties that require other specialized training.

(f) Annual refresher security education and training.

Agencies shall provide annual refresher training to employees who create, process, or handle classified information. Annual refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Annual refresher training should also address identification and handling of other agency-originated information and foreign government information, as well as the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Annual refresher training should also address issues or concerns identified during agency self-inspections.

(g) Termination briefings.
Except in extraordinary circumstances, each agency shall ensure that each employee who is granted access to classified information and who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn or revoked must receive such a briefing. At a minimum, termination briefings must impress upon each employee the continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance, and the obligation to return to the appropriate agency official all classified documents and materials in the employee’s possession.

(h) Other security education and training.

Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include:

(1) Practices applicable to U.S. officials traveling overseas;
(2) Procedures for protecting classified information processed and stored in automated information systems;
(3) Methods for dealing with uncleared personnel who work in proximity to classified information;
(4) Responsibilities of personnel serving as couriers of classified information; and
(5) Security requirements that govern participation in international programs.
SUBPART H—Standard Forms

(a) General.

The purpose of the standard forms is to promote the implementation of the government-wide information security program. Standard forms are prescribed when their use will enhance the protection of national security information and/or will reduce the costs associated with its protection. The use of the standard forms prescribed is mandatory for agencies of the executive branch that create or handle national security information. As appropriate, these agencies may mandate the use of these forms by their contractors, licensees, or grantees who are authorized access to national security information.

(b) Waivers.

Except for the SF 312, “Classified Information Nondisclosure Agreement,” and the SF 714, “Financial Disclosure Report,” (which are waiverable by the Director of National Intelligence, as the Security Executive Agent, under E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information) only the Director of ISOO may grant a waiver from the use of the prescribed standard forms. To apply for a waiver, an agency must submit its proposed alternative form to the Director of ISOO along with its justification for use. The Director of ISOO will review the request and notify the agency of the decision. Waivers approved prior to December 29, 2009, remain in effect and are subject to review.

(c) Availability.

Agencies may obtain copies of the standard forms prescribed by ordering through FEDSTRIP/MILSTRIP or from the GSA Consumer Global Supply Centers, or the GSA Advantage on-line service. Some of these standard forms can be downloaded from the GSA Forms Library.

(d) Standard Forms.

Standard forms required for application to national security information are as follows.

(1) **SF 311, Agency Security Classification Management Program Data:**
The SF 311 is a data collection form completed by only those executive branch agencies that create and/or handle classified national security information. The form is a record of classification management data provided by the agencies. The agencies submit the completed forms on an annual basis to ISOO, no later than November 15 following the reporting period, for inclusion in a report to the President.
(2) **SF 312, Classified Information Nondisclosure Agreement:**

(i) The SF 312 is a nondisclosure agreement between the United States and an employee of the Federal Government or one of its contractors, licensees, or grantees. The prior execution of this form by an individual is necessary before the United States Government may grant that individual access to classified information, with the exception of an emergency as defined in section 4.2(b) of the Order.

(ii) Electronic signatures on SF-312s are prohibited.

(iii) The SF 312 is the current authorized form; if an employee originally signed the now outdated SF 189 or SF 189-A, or a form under an approved waiver, as agreement to nondisclosure, the forms remain valid. The SF 189 and SF 189-A are no longer available for use with new employees.

(iv) The use of the “Security Debriefing Acknowledgement” portion of the SF 312 is optional at the discretion of the implementing agency. If an agency chooses not to record its debriefing by signing/dating the debriefing section of the SF 312, then the agency shall provide an alternative record.

(v) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee, or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.

(vi) The provisions of the SF 312, the SF 189, and the SF 189-A do not supersede the provisions of 5 U.S.C. 2302, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(vii) Each agency must retain its executed copies of the SF 312, SF 189, and SF 189-A in file systems from which an agreement can be expeditiously retrieved in the event that the United States must seek its enforcement or a subsequent employer must confirm its prior execution. The original, or a legally enforceable facsimile that is retained in lieu of the original, such as microfiche, microfilm, computer disk, or electronic storage medium, must be retained for 50 years following its date of execution. For agreements executed by civilian employees of the United States Government, an agency may store the executed copy of the SF 312 and SF 189 in the United States Office of Personnel Management's Official Personnel Folder as a long-term (right side) document for that employee. An agency may permit its contractors, licensees, and grantees to retain the executed agreements of their employees during the time of employment. Upon the termination of employment, the contractors, licensee, or grantee shall deliver the original or legally enforceable facsimile of the executed SF 312, SF 189, or SF 189-A of that employee to the Government agency primarily responsible for his or her classified work. A contractor, licensee, or grantee of an agency participating in the National Industrial Security Program shall provide the copy or legally enforceable facsimile of the executed SF 312, SF 189, or SF 189-A of a terminated employee to the

Page 1169
employee to their cognizant security office. Each agency shall inform ISOO of the
file systems that it uses to store these agreements for each category of affected
individuals.
(viii) Only the Director of National Intelligence, as the Security Executive Agent,
may grant an agency's request for a waiver from the use of the SF 312. To apply
for a waiver, an agency must submit its proposed alternative nondisclosure
agreement to the Director of the Special Security Center (SSC), Office of the
Director of National Intelligence, along with a justification for its use. The
Director, SSC, shall request a determination about the alternative agreement's
enforceability from the Department of Justice.
(ix) The national stock number for the SF 312 is 7540-01-280-5499.

(3) SF 700, Security Container Information:
The SF 700 provides the names, addresses, and telephone numbers of employees
who are to be contacted if the security container to which the form pertains is
found open and unattended. The form also includes the means to maintain a
current record of the security container's combination and provides the envelope
to be used to forward this information to the appropriate agency activity or
official. If an agency determines, as part of its risk management strategy, that a
security container information form is required, the SF 700 shall be used. Parts 2
and 2A of each completed copy of SF 700 shall be classified at the highest level of
classification of the information authorized for storage in the security container.
A new SF 700 must be completed each time the combination to the security
container is changed. The national stock number for the SF 700 is 7540-01-214-
5372.

(4) SF 701, Activity Security Checklist:
The SF 701 provides a systematic means to make a thorough end-of-day security
inspection for a particular work area and to allow for employee accountability in
the event that irregularities are discovered. If an agency determines, as part of its
risk management strategy, that an activity security checklist is required, the SF
701 will be used. Completion, storage, and disposition of SF 701 will be in
accordance with each agency's security regulations. The national stock number
for the SF 701 is 7540-01-213-7899.

(5) SF 702, Security Container Check Sheet:
The SF 702 provides a record of the names and times that persons have opened,
closed, or checked a particular container that holds classified information. If an
agency determines, as part of its risk management strategy, that a security
container check sheet is required, the SF 702 will be used. Completion, storage,
and disposal of the SF 702 will be in accordance with each agency's security
regulations. The national stock number of the SF 702 is 7540-01-213-7900.

(6) SF 703, TOP SECRET Cover Sheet:
The SF 703 serves as a shield to protect Top Secret classified information from
inadvertent disclosure and to alert observers that Top Secret information is
attached to it. If an agency determines, as part of its risk management strategy,
that a TOP SECRET cover sheet is required, the SF 703 will be used. The SF 703 is affixed to the top of the Top Secret document and remains attached until the document is downgraded, requiring the appropriate classification level cover sheet, declassified, or destroyed. When the SF 703 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 703 is 7540-01-213-7901.

(7) SF 704, SECRET Cover Sheet:
The SF 704 serves as a shield to protect Secret classified information from inadvertent disclosure and to alert observers that Secret information is attached to it. If an agency determines, as part of its risk management strategy, that a SECRET cover sheet is required, the SF 704 will be used. The SF 704 is affixed to the top of the Secret document and remains attached until the document is downgraded, requiring the appropriate classification level cover sheet, declassified, or destroyed. When the SF 704 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 704 is 7540-01-213-7902.

(8) SF 705, CONFIDENTIAL Cover Sheet:
The SF 705 serves as a shield to protect Confidential classified information from inadvertent disclosure and to alert observers that Confidential information is attached to it. If an agency determines, as part of its risk management strategy, that a CONFIDENTIAL cover sheet is required, the SF 705 will be used. The SF 705 is affixed to the top of the Confidential document and remains attached until the document is destroyed. When the SF 705 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 705 is 7540-01-213-7903.

(9) SF 706, TOP SECRET Label:
The SF 706 is used to identify and protect electronic media and other media that contain Top Secret information. The SF 706 is used instead of the SF 703 for media other than documents. If an agency determines, as part of its risk management strategy, that a TOP SECRET label is required, the SF 706 will be used. The SF 706 is affixed to the medium containing Top Secret information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 706 is 7540-01-207-5536.

(10) SF 707, SECRET Label:
The SF 707 is used to identify and protect electronic media and other media that contain Secret information. The SF 707 is used instead of the SF 704 for media other than documents. If an agency determines, as part of its risk management strategy, that a SECRET label is required, the SF 707 will be used. The SF 707 is affixed to the medium containing Secret information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 707 is 7540-01-207-5537.
(11) **SF 708, CONFIDENTIAL Label:**
The SF 708 is used to identify and protect electronic media and other media that contain Confidential information. The SF 708 is used instead of the SF 705 for media other than documents. If an agency determines, as part of its risk management strategy, that a CONFIDENTIAL label is required, the SF 708 will be used. The SF 708 is affixed to the medium containing Confidential information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 708 is 7540-01-207-5538.

(12) **SF 709, CLASSIFIED Label:**
The SF 709 is used to identify and protect electronic media and other media that contain classified information pending a determination by the classifier of the specific classification level of the information. If an agency determines, as part of its risk management strategy, that a CLASSIFIED label is required, the SF 709 will be used. The SF 709 is affixed to the medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. When a classifier has made a determination of the specific level of classification of the information contained on the medium, either the SF 706, SF 707, or SF 708 shall be affixed on top of the SF 709 so that only the SF 706, SF 707, or SF 708 is visible. The national stock number of the SF 709 is 7540-01-207-5540.

(13) **SF 710, UNCLASSIFIED Label:**
In a mixed environment in which classified and unclassified information are being processed or stored, the SF 710 is used to identify electronic media and other media that contain unclassified information. Its function is to aid in distinguishing among those media that contain either classified or unclassified information in a mixed environment. If an agency determines, as part of its risk management strategy, that an UNCLASSIFIED label is required, the SF 710 will be used. The SF 710 is affixed to the medium containing unclassified information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. However, the label is small enough so that it can be wholly covered by a SF 706, SF 707, SF 708, or SF 709 if the medium subsequently contains classified information. The national stock number of the SF 710 is 7540-01-207-5539.

(14) **SF 711, DATA DESCRIPTOR Label:**
The SF 711 is used to identify additional safeguarding controls that pertain to classified information that is stored or contained on electronic or other media. If an agency determines, as part of its risk management strategy, that a DATA DESCRIPTOR label is required, the SF 711 will be used. The SF 711 is affixed to the electronic medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. The SF 711 is ordinarily used in conjunction with the SF 706, SF 707, SF 708, or SF 709,
as appropriate. Once the label has been applied, it cannot be removed. The SF 711 provides spaces for information that should be completed as required. The national stock number of the SF 711 is 7540-01-207-5541.

(15) SF 714, Financial Disclosure Report:
When required by an agency head or by the Director of National Intelligence, as the Security Executive Agent, the SF 714 contains information that is used to make personnel security determinations, including whether to grant a security clearance; to allow access to classified information, sensitive areas, and equipment; or to permit assignment to sensitive national security positions. The data may later be used as a part of a review process to evaluate continued eligibility for access to classified information or as evidence in legal proceedings. The SF 714 assists law enforcement agencies in obtaining pertinent information in the preliminary stages of potential espionage and counter terrorism cases.

(16) SF 715, Government Declassification Review Tab:
The SF 715 is used to record the status of classified national security information reviewed for declassification. The SF 715 shall be used in all situations that call for the use of a tab as part of the processing of records determined to be of permanent historical value. The national stock number for the SF 715 is 7540-01-537-4689.
SUBPART I—Reporting and Definitions

(a) Delegations of original classification authority.

Agencies shall report delegations of original classification authority to ISOO annually in accordance with section 1.3(c) of the Order and § 2001.11(c).

(b) Statistical reporting.

Each agency that creates or safeguards classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

(c) Accounting for costs.

(1) Information on the costs associated with the implementation of the Order will be collected from the agencies. The agencies will provide data to ISOO on the cost estimates for classification-related activities. ISOO will report these cost estimates annually to the President. The agency senior official should work closely with the agency comptroller to ensure that the best estimates are collected.

(2) The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under E.O. 12829, as amended, National Industrial Security Program, and consistent with agreements entered into under section 202 of E.O. 12989, as amended, will collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO annually. ISOO will report these cost estimates annually to the President.

(d) Self-Inspections.

Agencies shall report annually to the Director of ISOO as required by section 5.4(d)(4) of the Order and outlined in § 2001.60(f).

32 CFR Section 2001.91: Other agency reporting requirements.

(a) Information declassified without proper authority.

Determinations that classified information has been declassified without proper authority shall be promptly reported in writing to the Director of ISOO in accordance with § 2001.13(a).

(b) Reclassification actions.

Reclassification of information that has been declassified and released under proper authority shall be reported promptly to the National Security Advisor and
the Director of ISOO in accordance with section 1.7(c)(3) of the Order and § 2001.13(b).

(c) Fundamental classification guidance review.

The initial fundamental guidance review is to be completed no later than June 27, 2012. Agency heads shall provide a detailed report summarizing the results of each classification guidance review to ISOO and release an unclassified version to the public in accordance with section 1.9 of the Order and § 2001.16(d).

(d) Violations of the Order.

Agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under sections 5.5(b)(1), (2), or (3) of the Order and § 2001.48(d).


(a) Accessioned records

means records of permanent historical value in the legal custody of NARA.

(b) Authorized person

means a person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know.

(c) Classification management

means the life-cycle management of classified national security information from original classification to declassification.

(d) Cleared commercial carrier

means a carrier that is authorized by law, regulatory body, or regulation, to transport Secret and Confidential material and has been granted a Secret facility clearance in accordance with the National Industrial Security Program.

(e) Control

means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(f) Employee

means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an
expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(g) Equity

refers to information:
(1) Originally classified by or under the control of an agency;
(2) In the possession of the receiving agency in the event of transfer of function; or
(3) In the possession of a successor agency for an agency that has ceased to exist.

(h) Exempted

means nomenclature and markings indicating information has been determined to fall within an enumerated exemption from automatic declassification under the Order.

(i) Facility

means an activity of an agency authorized by appropriate authority to conduct classified operations or to perform classified work.

(j) Federal record

includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference, and stocks of publications and processed documents are not included. (44 U.S.C. 3301)

(k) Newly discovered records

means records that were inadvertently not reviewed prior to the effective date of automatic declassification because the appropriate agency personnel were unaware of their existence.

(l) Open storage area

means an area constructed in accordance with § 2001.53 of this part and authorized by the agency head for open storage of classified information.
(m) Original classification authority with jurisdiction over the information
includes:
(1) The official who authorized the original classification, if that official is still serving in the same position;
(2) The originator’s current successor in function;
(3) A supervisory official of either; or
(4) The senior agency official under the Order.

(n) Permanent records
means any Federal record that has been determined by the National Archives to have sufficient value to warrant its preservation in the National Archives. Permanent records include all records accessioned by the National Archives into the National Archives and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by the National Archives on or after May 14, 1973.

(o) Permanently valuable information
or permanent historical value
refers to information contained in:
(1) Records that have been accessioned by the National Archives;
(2) Records that have been scheduled as permanent under a records disposition schedule approved by the National Archives; and
(3) Presidential historical materials, presidential records or donated historical materials located in the National Archives, a presidential library, or any other approved repository.

(p) Presidential papers, historical materials, and records
means the papers or records of the former Presidents under the legal control of the Archivist pursuant to sections 2111, 2111 note, or 2203 of title 44, U.S.C.

(q) Redaction
means the removal of classified information from copies of a document such that recovery of the information on the copy is not possible using any reasonably known technique or analysis.

(r) Risk management principles
means the principles applied for assessing threats and vulnerabilities and implementing security countermeasures while maximizing the sharing of information to achieve an acceptable level of risk at an acceptable cost.

(s) Security-in-depth
means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

(t) Supplemental controls

means prescribed procedures or systems that provide security control measures designed to augment the physical protection of classified information. Examples of supplemental controls include intrusion detection systems, periodic inspections of security containers or areas, and security-in-depth.

(u) Temporary records

means Federal records approved by NARA for disposal, either immediately or after a specified retention period. Also called disposable records.

(v) Transclassification

means information that has been removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable Executive orders as “National Security Information.”

(w) Unscheduled records

means Federal records whose final disposition has not been approved by NARA. All records that fall under a NARA approved records control schedule are considered to be scheduled records.
32 CFR PART 2003 [RESERVED]

32 CFR PART 2004—NATIONAL INDUSTRIAL SECURITY PROGRAM DIRECTIVE NO. 1

➢ Subpart A—Implementation and Oversight
  o 2004.5: Definitions.
  o 2004.10: Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].
  o 2004.11: Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].
  o 2004.12: Reviews by ISOO [102(b)(4)].

➢ Subpart B—Operations
  o 2004.20: National Industrial Security Program Operating Manual (NISPOM) [201(a)].
  o 2004.21: Protection of Classified Information [201(e)].
  o 2004.22: Operational Responsibilities [202(a)].
  o 2004.23: Cost Reports [203(d)].

Authority:

Source:
71 FR 18007, Apr. 10, 2006, unless otherwise noted.
SUBPART A—Implementation and Oversight
32 CFR Section 2004.5: Definitions.

(a) “Cognizant Security Agencies (CSAs)” means the Executive Branch departments and agencies authorized in EO 12829, as amended, to establish industrial security programs: The Department of Defense, designated as the Executive Agent; the Department of Energy; the Nuclear Regulatory Commission; and the Central Intelligence Agency.

(b) “Cognizant Security Office (CSO)” means the organizational entity delegated by the Head of a CSA to administer industrial security on behalf of the CSA.

(c) “Contractor” means any industrial, education, commercial, or other entity, to include licensees or grantees that has been granted access to classified information. Contractor does not include individuals engaged under personal services contracts.

(d) “National Interest Determination (NID)” means a determination that access to proscribed information is consistent with the national security interests of the United States.

(e) “Proscribed information” means Top Secret; Communications Security, except classified keys used for data transfer; Restricted Data; Special Access Program; or Sensitive Compartmented Information.

[71 FR 18007, Apr. 10, 2006. Redesignated and amended at 75 FR 17306, Apr. 6, 2010]

32 CFR Section 2004.10: Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].

Bracketed references pertain to related sections of Executive Order 12829, as amended by E.O. 12885.

The Director ISOO shall:

(a) Implement EO 12829, as amended.

(b) Ensure that the NISP is operated as a single, integrated program across the Executive Branch of the Federal Government; i.e., that the Executive Branch departments and agencies adhere to NISP principles.

(c) Ensure that each contractor’s implementation of the NISP is overseen by a single Cognizant Security Authority (CSA), based on a preponderance of classified contracts per agreement by the CSAs.

(d) Ensure that all Executive Branch departments and agencies that contract for classified work have included the Security Requirements clause, 52.204-2, from the Federal Acquisition Regulation (FAR), or an equivalent clause, in such contract.

(e) Ensure that those Executive Branch departments and agencies for which the Department of Defense (DoD) serves as the CSA have entered into agreements with the DoD that establish the terms of the Secretary’s responsibilities on behalf of those agency heads.
32 CFR Section 2004.11: Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].

(a) Reviews and Updates.

All implementing regulations, internal rules, or guidelines that pertain to the NISP shall be reviewed and updated by the originating agency, as circumstances require. If a change in national policy necessitates a change in agency implementing regulations, internal rules, or guidelines that pertain to the NISP, the agency shall promptly issue revisions.

(b) Reviews by ISOO.

The Director, ISOO, shall review agency implementing regulations, internal rules, or guidelines, as necessary, to ensure consistency with NISP policies and procedures. Such reviews should normally occur during routine oversight visits, when there is indication of a problem that comes to the attention of the Director, ISOO, or after a change in national policy that impacts such regulations, rules, or guidelines. The Director, ISOO, shall provide findings from such reviews to the responsible department or agency.

32 CFR Section 2004.12: Reviews by ISOO [102(b)(4)].
The Director, ISOO, shall fulfill his monitoring role based, in part, on information received from NISP Policy Advisory Committee (NISPPAC) members, from on-site reviews that ISOO conducts under the authority of EO 12829, as amended, and from complaints and suggestions from persons within or outside the Government. Findings shall be reported to the responsible department or agency.
SUBPART B—Operations
(a) The NISPOM applies to release of classified information during all phases of the contracting process.
(b) As a general rule, procedures for safeguarding classified information by contractors and recommendations for changes shall be addressed through the NISPOM coordination process that shall be facilitated by the Executive Agent. The Executive Agent shall address NISPOM issues that surface from industry, Executive Branch departments and agencies, or the NISPPAC. When consensus cannot be achieved through the NISPOM coordination process, the issue shall be raised to the NSC for resolution.

32 CFR Section 2004.21: Protection of Classified Information [201(e)].
Procedures for the safeguarding of classified information by contractors are promulgated in the NISPOM. DoD, as the Executive Agent, shall use standards applicable to agencies as the basis for the requirements, restrictions, and safeguards contained in the NISPOM; however, the NISPOM requirements may be designed to accommodate as necessary the unique circumstances of industry. Any issue pertaining to deviation of industry requirements in the NISPOM from the standards applicable to agencies shall be addressed through the NISPOM coordination process.

32 CFR Section 2004.22: Operational Responsibilities [202(a)].
(a) Designation of Cognizant Security Authority (CSA).

The CSA for a contractor shall be determined by the preponderance of classified contract activity per agreement by the CSAs. The responsible CSA shall conduct oversight inspections of contractor security programs and provide other support services to contractors as necessary to ensure compliance with the NISPOM and that contractors are protecting classified information as required. DoD, as Executive Agent, shall serve as the CSA for all Executive Branch departments and agencies that are not a designated CSA. As such, DoD shall:
(1) Provide training to industry to ensure that industry understands the responsibilities associated with protecting classified information.
(2) Validate the need for contractor access to classified information, shall establish a system to request personnel security investigations for contractor personnel, and shall ensure adequate funding for investigations of those contractors under Department of Defense cognizance.
(3) Maintain a system of eligibility and access determinations of contractor personnel.

(b) General Responsibilities.
Executive Branch departments and agencies that issue contracts requiring industry to have access to classified information and are not a designated CSA shall:
(1) Include the Security Requirements clause, 52.204-2, from the FAR in such contracts;
(2) Incorporate a Contract Security Classification Specification (DD 254) into the contracts in accordance with the FAR subpart 4.4;
(3) Sign agreements with the Department of Defense as the Executive Agent for industrial security services; and,
(4) Ensure applicable department and agency personnel having NISP implementation responsibilities are provided appropriate education and training.

(c) National Interest Determinations (NIDs).

Executive branch departments and agencies shall make a National Interest Determination (NID) before authorizing contractors, cleared or in process for clearance under a Special Security Agreement (SSA), to have access to proscribed information. To make a NID, the agency shall assess whether release of the proscribed information is consistent with the national security interests of the United States.
(1) The requirement for a NID applies to new contracts, including pre-contract activities in which access to proscribed information is required, and to existing contracts when contractors are acquired by foreign interests and an SSA is the proposed foreign ownership, control, or influence mitigation method.
(i) If access to proscribed information is required to complete pre-contract award actions or to perform on a new contract, the Government Contracting Activity (GCA) shall determine if release of the information is consistent with national security interests.
(ii) For contractors that have existing contracts that require access to proscribed information, have been or are in the process of being acquired by foreign interests, and have proposed an SSA to mitigate foreign ownership, the Cognizant Security Agency (CSA), or when delegated, the Cognizant Security Office (CSO) shall notify the GCA of the need for a NID.
(iii) The GCA(s) shall determine, within 30 days, per § 2004.22(c)(4)(i), or 60 days, per § 2004.22(c)(4)(ii), whether release of the proscribed information is consistent with national security interests unless the GCA requires additional time for the NID process due to special circumstances. The GCA shall formally advise the CSA, if special circumstances apply.
(2) In accordance with 10 U.S.C. 2536, DoD and the Department of Energy (DOE) cannot award a contract involving access to proscribed information to a contractor effectively owned or controlled by a foreign government unless a waiver has been issued by the Secretary of Defense or Secretary of Energy.
(3) NIDs may be program-, project-, or contract-specific. For program and project NIDs, a separate NID is not required for each contract. The CSO may require the GCA to identify all contracts covered by the NID. NID decisions shall
be made by officials as specified by CSA policy or as designated by the agency head.

(4) NID decisions shall be made within 30 days.

(i) Where no interagency coordination is required because the department or agency owns or controls all of the proscribed information in question, the GCA shall provide a final documented decision to the applicable CSO, with a copy to the contractor, within 30 days of the date of the request for the NID.

(ii) If the proscribed information is owned by, or under the control of, a department or agency other than the GCA (e.g., National Security Agency (NSA) for Communications Security, the Office of the Director of National Intelligence (ODNI) for Sensitive Compartmented Information, and DOE for Restricted Data), the GCA shall provide written notice to that department or agency that its written concurrence is required. Such notice shall be provided within 30 days of being informed by the CSO of the requirement for a NID. The GCA shall provide a final documented decision to the applicable CSO, with a copy to the contractor, within 60 days of the date of the request for the NID.

(iii) If the NID decision is not provided within 30 days, per § 2004.22(c)(4)(i), or 60 days, per § 2004.22(c)(4)(ii), the CSA shall intercede to request the GCA to provide a decision. In such instances, the GCA, in addition to formally notifying the CSA of the special circumstances, per § 2004.22(c)(1)(iii), will provide the CSA or its designee with updates at 30-day intervals. The CSA, or its designee, will, in turn, provide the contractor with updates at 30-day intervals until the NID decision is made.

(5) The CSO shall not delay implementation of an SSA pending completion of a GCA’s NID processing, provided there is no indication that a NID will be denied either by the GCA or the owner of the information (i.e., NSA, DOE, or ODNI). However, the contractor shall not have access to additional proscribed information under a new contract until the GCA determines that the release of the information is consistent with national security interests and issues a NID.

(6) The CSO shall not upgrade an existing contractor clearance under an SSA to Top Secret unless an approved NID covering the prospective Top Secret access has been issued.

[71 FR 18007, Apr. 10, 2006 as amended at 75 FR 17306, Apr. 6, 2010]

32 CFR Section 2004.23: Cost Reports [203(d)].

(a) The Executive Branch departments and agencies shall provide information each year to the Director, ISOO, on the costs within the agency associated with implementation of the NISP for the previous year.

(b) The DoD as the Executive Agent shall develop a cost methodology in coordination with industry to collect the costs incurred by contractors of all Executive Branch departments and agencies to implement the NISP, and shall report those costs to the Director, ISOO, on an annual basis.

Page 1184
32 CFR CHAPTER XXI—NATIONAL SECURITY COUNCIL

32 CFR PART 2102—RULES AND REGULATIONS TO IMPLEMENT THE PRIVACY ACT OF 1974

- 2102.1: Introduction.
- 2102.2: Purpose and scope.
- 2102.3: Definitions.
- 2102.4: Procedures for determining if an individual is the subject of a record.
- 2102.13: Requirements for access to a record.
- 2102.15: Requirements for requests to amend records.
- 2102.21: Procedures for appeal of determination to deny access to or amendment of requested records.
- 2102.31: Disclosure of a record to persons other than the individual to whom it pertains.
- 2102.41: Fees.
- 2102.51: Penalties.
- 2102.61: Exemptions.

Authority:
5 U.S.C. 552a (f) and (k).

Source:
40 FR 47746, Oct. 9, 1975, unless otherwise noted.

32 CFR Section 2102.1: Introduction.
(a) Insofar as the Privacy Act of 1974 (5 U.S.C. 552a) applies to the National Security Council (hereafter NSC), it provides the American public with expanded opportunities to gain access to records maintained by the NSC Staff which may pertain to them as individuals. These regulations are the exclusive means by which individuals may request personally identifiable records and information from the National Security Council.
(b) The NSC Staff, in addition to performing the functions prescribed in the National Security Act of 1947, as amended (50 U.S.C. 401), also serves as the supporting staff to the President in the conduct of foreign affairs. In doing so the NSC Staff is acting not as an agency but as an extension of the White House Office. In that the White House Office is not considered an agency for the purposes of this Act, the materials which are used by NSC Staff personnel in their role as supporting staff to the President are not subject to the provisions of the
Privacy Act of 1974. A description of these White House Office files is, nevertheless, appended to the NSC notices of systems of files and will be published annually in the Federal Register.

c) In general, Records in NSC files pertain to individual members of the public only if these individuals have been (1) employed by the NSC, (2) have corresponded on a foreign policy matter with a member of the NSC or its staff, or (3) have, as a U.S. Government official, participated in an NSC meeting or in the preparation of foreign policy-related documents for the NSC.

32 CFR Section 2102.2: Purpose and scope.
(a) The following regulations set forth procedures whereby individuals may seek and gain access to records concerning themselves and will guide the NSC Staff response to requests under the Privacy Act. In addition, they outline the requirements applicable to the personnel maintaining NSC systems of records.
(b) These regulations, published pursuant to the Privacy Act of 1974, Pub. L. 93-579, Section 552a (f) and (k), 5 U.S.C. (hereinafter the Act), advise of procedures whereby an individual can:
(1) Request notification of whether the NSC Staff maintains or has disclosed a record pertaining to him or her in any non-exempt system of records;
(2) Request a copy of such record or an accounting of that disclosure;
(3) Request an amendment to a record; and,
(4) Appeal any initial adverse determination of any request under the Act.
(c) These regulations also specify those systems of records which the NSC has determined to be exempt from certain provisions of the Act and thus not subject to procedures established by this regulation.

32 CFR Section 2102.3: Definitions.
As used in these regulations:

(a) Individual.
A citizen of the United States or an alien lawfully admitted for permanent residence.

(b) Maintain.
Includes maintain, collect, use or disseminate. Under the Act it is also used to connote control over, and, therefore, responsibility for, systems of records in support of the NSC statutory function (50 U.S.C. 401, et seq.).

(c) Systems of Records.
A grouping of any records maintained by the NSC from which information is retrieved by the name of the individual or by some other identifying particular assigned to the individual.
Any decision made by the NSC or designated official thereof which affects the individual's rights, opportunities, benefits, etc. and which is based in whole or in part on information contained in that individual's record.

(e) Routine Use.

With respect to the disclosure of a record, the use of such a record in a manner which is compatible with the purpose for which it was collected.

(f) Disclosure.

The granting of access or transfer of a record by any means.

32 CFR Section 2102.4: Procedures for determining if an individual is the subject of a record.

(a) Individuals desiring to determine if they are the subject of a record or system of records maintained by the NSC Staff should address their inquiries, marking them plainly as a PRIVACY ACT REQUEST, to:

Staff Secretary, National Security Council, Room 374, Old Executive Office Building, Washington, DC 20506.

All requests must be made in writing and should contain:
(1) A specific reference to the system of records maintained by the NSC as listed in the NSC Notices of Systems and Records (copies available upon request); or
(2) A description of the record or systems of records in sufficient detail to allow the NSC to determine whether the record does, in fact, exist in an NSC system of records.

(b) All requests must contain the printed or typewritten name of the individual to whom the record pertains, the signature of the individual making the request, and the address to which the reply should be sent. In instances when the identification is insufficient to insure disclosure to the individual to whom the information pertains in view of the sensitivity of the information, NSC reserves the right to solicit from the requestor additional identifying information.

(c) Responses to all requests under the Act will be made by the Staff Secretary, or by another designated member of the NSC Staff authorized to act in the name of the Staff Secretary in responding to a request under this Act. Every effort will be made to inform the requestor if he or she is the subject of a specific record or system of records within ten working days (excluding Saturdays, Sundays and legal Federal Holidays) of receipt of the request. Such a response will also contain the procedures to be followed in order to gain access to any record which may exist and a copy of the most recent NSC notice, as published in the Federal Register, on the system of records in which the record is contained.

(d) Whenever it is not possible to respond in the time period specified above, the NSC Staff Secretary or a designated alternate will, within ten working days
(excluding Saturdays, Sundays and legal Federal Holidays), inform the requestor of the reasons for the delay (e.g., insufficient requestor information, difficulties in record location, etc.), steps that need to be taken in order to expedite the request, and the date by which a response is anticipated.

32 CFR Section 2102.13: Requirements for access to a record.
(a) Individuals requesting access to a record or system of records in which there is information concerning them must address a request in writing to the Staff Secretary of the NSC (see § 2102.1). Due to restricted access to NSC offices in the Old Executive Office Building where the files are located, requests cannot be made in person.
(b) All written requests should contain a concise description of the records to which access is requested. In addition, the requestor should include any other information which he or she feels would assist in the timely identification of the record. Verification of the requestor’s identity will be determined under the same procedures used in requests for learning of the existence of a record.
(c) To the extent possible, any request for access will be answered by the Staff Secretary or a designated alternate within ten working days (excluding Saturdays, Sundays, and legal Federal holidays) of the receipt of the request. In the event that a response cannot be made within this time, the requestor will be notified by mail of the reasons for the delay and the date upon which a reply can be expected.
(d) The NSC response will forward a copy of the requested materials unless further identification or clarification of the request is required. In the event access is denied, the requestor shall be informed of the reasons therefore and the name and address of the individual to whom an appeal should be directed.

32 CFR Section 2102.15: Requirements for requests to amend records.
(a) Individuals wishing to amend a record contained in the NSC systems of records pertaining to them must submit a request in writing to the Staff Secretary of the NSC in accordance with the procedures set forth herein.
(b) All requests for amendment or correction of a record must state concisely the reason for requesting the amendment. Such requests should include a brief statement which describes the information the requestor believes to be inaccurate, incomplete, or unnecessary and the amendment or correction desired.
(c) To the extent possible, every request for amendment of a record will be answered within ten working days (excluding Saturdays, Sundays, and legal Federal holidays) of the receipt of the request. In the event that a response cannot be made within this time, the requestor will be notified by mail of the reasons for the delay and the date upon which a reply can be expected. A final response to a request for amendment will include the NSC Staff determination on whether to grant or deny the request. If the request is denied, the response will include:
(1) The reasons for the decision;
(2) The name and address of the individual to whom an appeal should be directed;
(3) A description of the process for review of the appeal within the NSC; and
(4) A description of any other procedures which may be required of the individual
in order to process the appeal.

32 CFR Section 2102.21: Procedures for appeal of determination to
deny access to or amendment of requested records.
(a) Individuals wishing to appeal an NSC Staff denial of a request for access or to
amend a record concerning them must address a letter of appeal to the Staff
Secretary of the NSC. The letter must be received within thirty days from the date
of the Staff Secretary’s notice of denial and, at a minimum, should identify the
following:
(1) The records involved;
(2) The dates of the initial request and subsequent NSC determination; and
(3) A brief statement of the reasons supporting the request for reversal of the
adverse determination.
(b) Within thirty working days (excluding Saturdays, Sundays and legal Federal
holidays) of the date of receipt of the letter of appeal, the Assistant to the
President for National Security Affairs (hereinafter the “Assistant”), or the
Deputy Assistant to the President for National Security Affairs (hereinafter the
“Deputy Assistant”), acting in his name, shall issue a determination on the
appeal. In the event that a final determination cannot be made within this time
period, the requestor will be informed of the delay, the reasons therefor and the
date on which a final response is expected.
(c) If the original request was for access and the initial determination is reversed,
a copy of the records sought will be sent to the individual. If the initial
determination is upheld, the requestor will be so advised and informed of the
right to judicial review pursuant to 5 U.S.C. 552a(g).
(d) If the initial denial of a request to amend a record is reversed, the records will
be corrected and a copy of the amended record will be sent to the individual. In
the event the original decision is upheld by the Assistant to the President, the
requestor will be so advised and informed in writing of his or her right to seek
judicial review of the final agency determination, pursuant to section 552a(g) of
title 5, U.S.C. In addition, the requestor will be advised of his right to have a
concise statement of the reasons for disagreeing with the final determination
appended to the disputed records. This statement should be mailed to the Staff
Secretary within ten working days (excluding Saturdays, Sundays, and legal
Federal Holidays) of the date of the requestor’s receipt of the final determination.

32 CFR Section 2102.31: Disclosure of a record to persons other
than the individual to whom it pertains.
(a) Except as provided by the Privacy Act, 5 U.S.C. 552a(b), the NSC will not
disclose a record concerning an individual to another person or agency without
the prior written consent of the individual to whom the record pertains.

32 CFR Section 2102.41: Fees.
(a) Individuals will not be charged for:
(1) The first copy of any record provided in response to a request for access or amendment;
(2) The search for, or review of, records in NSC files;
(3) Any copies reproduced as a necessary part of making a record or portion thereof available to the individual.
(b) After the first copy has been provided, records will be reproduced at the rate of twenty-five cents per page for all copying of four pages or more.
(c) The Staff Secretary may provide copies of a record at no charge if it is determined to be in the interest of the Government.
(d) The Staff Secretary may require that all fees be paid in full prior to the issuance of the requested copies.
(e) Remittances shall be in the form of a personal check or bank draft drawn on a bank in the United States, or a postal money order. Remittances shall be made payable to the “United States Treasury” and mailed to the Staff Secretary, National Security Council, Washington, DC 20506.
(f) A receipt for fees paid will be given only upon request. Refund of fees paid for services actually rendered will not be made.

32 CFR Section 2102.51: Penalties.
Title 18, U.S.C. section 1001, Crimes and Criminal Procedures, makes it a criminal offense, subject to a maximum fine of $10,000 or imprisonment for not more than five years or both, to knowingly and willfully make or cause to be made any false or fraudulent statements or representations in any matter within the jurisdiction of any agency of the United States. Section (i)(3) of the Privacy Act (5 U.S.C. 552a) makes it a misdemeanor, subject to a maximum fine of $5,000, to knowingly and willfully request or obtain any record concerning an individual under false pretenses. Sections (i)(1) and (2) of 5 U.S.C. 552a provide penalties for violations by agency employees, of the Privacy Act or regulations established thereunder.

32 CFR Section 2102.61: Exemptions.
Pursuant to subsection (k) of the Privacy Act (5 U.S.C. 552a), the Staff Secretary has determined that certain NSC systems of records may be exempt in part from sections 553(c)(3), (d), (e)(1), (e)(4), (G), (H), (I), and (f) of title 5, and from the provisions of these regulations. These systems of records may contain information which is classified pursuant to Executive Order 11652. To the extent that this occurs, records in the following systems would be exempt under the provision of 5 U.S.C. 552a(k)(1):
NSC 1.1—Central Research Index,
NSC 1.2—NSC Correspondence Files, and
NSC 1.3—NSC Meetings Registry.
32 CFR PART 2103—REGULATIONS TO IMPLEMENT E.O. 12065—INCLUDING PROCEDURES FOR PUBLIC ACCESS TO DOCUMENTS THAT MAY BE DECLASSIFIED

➢ Subpart A—Introduction
  o 2103.1: References.
  o 2103.2: Purpose.
  o 2103.3: Applicability.
➢ Subpart B—Original Classification
  o 2103.11: Basic policy.
  o 2103.12: Level of original classification.
  o 2103.13: Duration of original classification.
  o 2103.14: Challenges to classification.
➢ Subpart C—Derivative Classification
  o 2103.21: Definition and application.
➢ Subpart D—Declassification and Downgrading
  o 2103.31: Declassification authority.
  o 2103.32: Mandatory review for declassification.
  o 2103.33: Downgrading authority.
➢ Subpart E—Safeguarding
  o 2103.41: Reproduction controls.
➢ Subpart F—Implementation and Review
  o 2103.51: Information Security Oversight Committee.
  o 2103.52: Classification Review Committee.

Authority:

Source:
44 FR 2384, Jan. 11, 1979, unless otherwise noted.
SUBPART A—Introduction

32 CFR Section 2103.1: References.

32 CFR Section 2103.2: Purpose.
The purpose of this regulation is to ensure, consistent with the authorities listed in § 2103.1, that national security information processed by the National Security Council Staff is protected from unauthorized disclosure, but only to the extent, and for such period, as is necessary to safeguard the national security.

32 CFR Section 2103.3: Applicability.
This regulation governs the National Security Council Staff Information Security Program. In consonance with the authorities listed in § 2103.1, it establishes the policy and procedures for the security classification, downgrading, declassification, and safeguarding of information that is owned by, is produced for or by, or is under the control of the National Security Council Staff.
SUBPART B—Original Classification

32 CFR Section 2103.11: Basic policy.
It is the policy of the National Security Council Staff to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security.

32 CFR Section 2103.12: Level of original classification.
Unnecessary classification, and classification at a level higher than is necessary, shall be avoided. If there is reasonable doubt as to which designation in section 1-1 of Executive Order 12065 is appropriate, or whether information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

32 CFR Section 2103.13: Duration of original classification.
Original classification may be extended beyond six years only by officials with Top Secret classification authority. This extension authority shall be used only when these officials determine that the basis for original classification will continue throughout the entire period that the classification will be in effect and only for the following reasons:
(a) The information is “foreign government information” as defined by the authorities in § 2301.1;
(b) The information reveals intelligence sources and methods;
(c) The information pertains to communication security;
(d) The information reveals vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to render ineffective a system, installation, or project important to the national security;
(e) The information concerns plans important to the national security, the unauthorized disclosure of which reasonably can be expected to nullify the effectiveness of the plan;
(f) The information concerns specific foreign relations matters, the continued protection of which is essential to the national security;
(g) Disclosure of the information would place a person's life in immediate jeopardy; or
(h) The continued protection of the information is specifically required by statute.

Even when the extension authority is exercised, the period of original classification shall not be greater than twenty years from the date of original classification, except that the original classification of “foreign government information” pursuant to paragraph (a) of this section may be for a period of thirty years.

32 CFR Section 2103.14: Challenges to classification.
If holders of classified information believe that the information is improperly or unnecessarily classified, or that original classification has been extended for too long a period, they should discuss the matter with their immediate superiors or
the classifier of the information. If these discussions do not satisfy the concerns of the challenger, the matter should be brought to the attention of the chairperson of the NSC Information Security Oversight Committee (see § 2103.51 of this part).
32 CFR Section 2103.21: Definition and application. Derivative classification is the act of assigning a level of classification to information that is determined to be the same in substance as information that is currently classified. Thus, derivative classification may be accomplished by any person cleared for access to that level of information, regardless of whether the person has original classification authority at that level.
SUBPART D—Declassification and Downgrading

32 CFR Section 2103.31: Declassification authority.
The Staff Secretary, Staff Counsel, and Director of Freedom of Information of the National Security Council Staff are authorized to declassify NSC documents after consultation with the appropriate NSC Staff members.

32 CFR Section 2103.32: Mandatory review for declassification.

(a) Receipt.

(1) Requests for mandatory review for declassification under section 3-501 of Executive Order 12065 must be in writing and should be addressed to:

National Security Council, ATTN: Staff Secretary (Mandatory Review Request), Old Executive Office Building, Washington, DC 20506.

(2) The requestor shall be informed of the date of receipt of the request. This date will be the basis for the time limits specified in paragraph (b) of this section.

(3) If the request does not reasonably describe the information sought, the requestor shall be notified that, unless additional information is provided or the request is made more specific, no further action will be taken.

(b) Review.

(1) The requestor shall be informed of the National Security Council Staff determination within sixty days of receipt of the initial request.

(2) If the determination is to withhold some or all of the material requested, the requestor may appeal the determination. The requestor shall be informed that such an appeal must be made in writing within sixty days of receipt of the denial and should be addressed to the chairperson of the National Security Council Classification Review Committee.

(3) The requestor shall be informed of the appellate determination within thirty days of receipt of the appeal.

(c) Fees.

(1) Fees for the location and reproduction of information that is the subject of a mandatory review request shall be assessed according to the following schedule:

(i) Search for records.
$5.00 per hour when the search is conducted by a clerical employee; $8.00 per hour when the search is conducted by a professional employee. No fee shall be assessed for searches of less than one hour.
(ii) Reproduction of documents.
Documents will be reproduced at a rate of $.25 per page for all copying of four pages or more. No fee shall be assessed for reproducing documents that are three pages or less, or for the first three pages of longer documents.

(2) Where it is anticipated that the fees chargeable under this section will amount to more than $25, and the requestor has not indicated in advance a willingness to pay fees as high as are anticipated, the requestor shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by the NSC Staff until a reply is received from the requestor.

(3) Remittances shall be in the form either of a personal check or bank draft drawn on a bank in the United States, or a postal money order. Remittances shall be made payable to the Treasury of the United States and mailed to the Staff Secretary, National Security Council, Washington, DC 20506.

(4) [Reserved]

(5) A receipt for fees paid will be given only upon request. Refund of fees paid for services actually rendered will not be made.

(6) If a requestor fails to pay within thirty days for services rendered, further action on any other requests submitted by that requestor shall be suspended.

(7) The Staff Secretary, National Security Council may waive all or part of any fee provided for in this section when it is deemed to be in either the interest of the NSC Staff or of the general public.

32 CFR Section 2103.33: Downgrading authority.
The Staff Secretary, Staff Counsel, and Director of Freedom of Information of the National Security Council Staff are authorized to downgrade NSC documents, after consultation with the appropriate NSC Staff members.
SUBPART E—Safeguarding
32 CFR Section 2103.41: Reproduction controls.
The Staff Secretary shall maintain records to show the number and distribution
of all Top Secret documents, of all documents covered by special access programs
distributed outside the originating agency, and of all Secret and Confidential
documents that are marked with special dissemination or reproduction
limitations.
SUBPART F—Implementation and Review

The NCS Information Security Oversight Committee shall be chaired by the Staff Counsel of the National Security Council Staff. The Committee shall be responsible for acting on all suggestions and complaints concerning the administration of the National Security Council information security program. The chairperson, who shall represent the NSC Staff on the Interagency Information Security Committee shall also be responsible for conducting an active oversight program to ensure effective implementation of Executive Order 12065.

32 CFR Section 2103.52: Classification Review Committee.
The NSC Classification Review Committee shall be chaired by the Staff Secretary of the National Security Council. The Committee shall decide appeals from denials of declassification requests submitted pursuant to section 3-5 of Executive Order 12065. The Committee shall consist of the chairperson, the NSC Director of Freedom of Information, and the NSC Staff member with primary subject matter responsibility for the material under review.
Subpart A—General Provisions
  o 2400.1: Authority.
  o 2400.2: Purpose.
  o 2400.3: Applicability.
  o 2400.4: Atomic Energy Material.
Subpart B—Original Classification
  o 2400.5: Basic policy.
  o 2400.6: Classification levels.
  o 2400.7: Original classification authority.
  o 2400.8: Limitations on delegation of original classification authority.
  o 2400.9: Classification requirements.
  o 2400.10: Presumption of damage.
  o 2400.11: Duration of classification.
  o 2400.12: Identification and markings.
  o 2400.13: Limitations on classification.
Subpart C—Derivative Classification
  o 2400.14: Use of derivative classification.
  o 2400.15: Classification guides.
  o 2400.16: Derivative classification markings.
Subpart D—Declassification and Downgrading
  o 2400.17: Policy.
  o 2400.18: Declassification and downgrading authority.
  o 2400.19: Declassification by the Director of the Information Security Oversight Office.
  o 2400.20: Systematic review for declassification.
  o 2400.21: Mandatory review for declassification.
  o 2400.23: Prohibition.
  o 2400.24: Downgrading.
Subpart E—Safeguarding
  o 2400.25: Access.
- 2400.26: Access by historical researchers and former Presidential appointees.
- 2400.27: Storage of classification information.
- 2400.28: Dissemination of classified information.
- 2400.29: Accountability and control.
- 2400.30: Reproduction of classified information.
- 2400.31: Destruction of classified information.
- 2400.32: Transmittal of classified information.
- 2400.33: Loss or possible compromise.

- Subpart F—Foreign Government Information
  - 2400.34: Classification.
  - 2400.35: Duration of classification.
  - 2400.36: Declassification.
  - 2400.37: Mandatory review.
  - 2400.38: Protection of foreign government information.

- Subpart G—Security Education
  - 2400.39: Responsibility and objectives.

- Subpart H—Office of Science and Technology Policy Information Security Program Management
  - 2400.40: Responsibility.
  - 2400.41: Office Review Committee.
  - 2400.42: Security Officer.
  - 2400.43: Heads of offices.
  - 2400.44: Custodians.
  - 2400.45: Information Security Program Review.
  - 2400.46: Suggestions or complaints.

**Authority:**

**Source:**
48 FR 10821, Mar. 15, 1983, unless otherwise noted.
SUBPART A—General Provisions

32 CFR Section 2400.1: Authority.


32 CFR Section 2400.2: Purpose.
The purpose of this Regulation is to ensure, consistent with the authorities of § 2400.1 that information of the Office of Science and Technology Policy (OSTP) relating to national security is protected from unauthorized disclosure, but only to the extent and for such period as is necessary to safeguard the national security.

32 CFR Section 2400.3: Applicability.
This Regulation governs the Office of Science and Technology Policy Information Security Program. In accordance with the provisions of Executive Order 12356 and Directive No. 1 it establishes, for uniform application throughout the Office of Science and Technology Policy, the policies and procedures for the security classification, downgrading, declassification and safeguarding of information that is owned by, produced for or by, or under the control of the office of Science and Technology Policy.

Nothing in this Regulation supersedes any requirement made by or under the Atomic Energy act of 1954, as amended. “Restricted Data” and information designated as “Formerly Restricted Data” shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto by the Department of Energy.
SUBPART B—Original Classification

32 CFR Section 2400.5: Basic policy.

Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, as implemented by Directive No. 1 and this Regulation, provides the only basis for classifying information. The policy of the Office of Science and Technology Policy is to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security. Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security.

32 CFR Section 2400.6: Classification levels.

(a) National security information (hereinafter “classified information”) shall be classified at one of the following three levels:

(1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information. Markings other than “Top Secret,” “Secret,” and “Confidential,” such as “For Official Use Only,” shall not be used to identify national security information. In addition, no other term or phrase shall be used in conjunction with one of the three authorized classification levels, such as “Secret Sensitive” or “Agency Confidential.” The terms “Top Secret”, “Secret”, and “Confidential” should not be used to identify nonclassified executive branch information.

(c) Unnecessary classification, and classification at a level higher than is necessary shall be scrupulously avoided.

(d) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified “Confidential” pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification the originator of the information shall safeguard it at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days. Upon the determination of a need for classification and/or the proper classification level, the information that is classified shall be marked as provided in § 2400.12 of this part.

32 CFR Section 2400.7: Original classification authority.

(a) Authority for original classification of information as Top Secret shall be exercised within OSTP only by the Director and by such principal subordinate officials having frequent need to exercise such authority as the Director shall designate in writing.
(b) The authority to classify information originally as Secret shall be exercised within OSTP only by the Director, other officials delegated in writing to have original Top Secret classification authority, and any other officials delegated in writing to have original Secret classification authority.

(c) The authority to classify information originally as Confidential shall be exercised within OSTP only by officials with original Top Secret or Secret classification authority and any officials delegated in writing to have original Confidential classification authority.

32 CFR Section 2400.8: Limitations on delegation of original classification authority.
(a) The Director, OSTP is the only official authorized to delegate original classification authority.
(b) Delegations of original classification authority shall be held to an absolute minimum.
(c) Delegations of original classification authority shall be limited to the level of classification required.
(d) Original classification authority shall not be delegated to OSTP personnel who only quote, restate, extract or paraphrase, or summarize classified information or who only apply classification markings derived from source material or as directed by a classification guide.
(e) The Executive Director, OSTP, shall maintain a current listing of persons or positions receiving any delegation of original classification authority. If possible, this listing shall be unclassified.
(f) Original classification authority may not be redelegated.
(g) Exceptional Cases.
When an employee, contractor, licensee, or grantee of OSTP that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with these Regulations as provided in § 2400.6(d) of this part. The information shall be transmitted promptly as provided in these Regulations to the official in OSTP who has appropriate subject matter interest and classification authority with respect to this information. That official shall decide within thirty (30) days whether to classify this information. If the information is not within OSTP’s area of classification responsibility, OSTP shall promptly transmit the information to the responsible agency. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

32 CFR Section 2400.9: Classification requirements.
(a) Information may be classified only if it concerns one or more of the categories cited in Executive Order 12356, as subcategorized below, and an official having original classification authority determines that its unauthorized disclosure,
either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(1) Military plans, weapons or operations;
(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
(3) Foreign government information;
(4) Intelligence activities (including special activities), or intelligence sources or methods;
(5) Foreign relations or foreign activities of the United States;
(6) Scientific, technological, or economic matters relating to the national security;
(7) United States Government programs for safe-guarding nuclear materials or facilities;
(8) Cryptology;
(9) A confidential source; or
(10) Other categories of information which are related to national security and that require protection against unauthorized disclosure as determined by the Director, Office of Science and Technology Policy. Each such determination shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Foreign government information need not fall within any other classification category listed in paragraph (a) of this section to be classified.

(c) Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be fully supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(d) Information classified in accordance with this section shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with Executive Order 12356 or predecessor orders, OSTP, if the agency of primary interest, shall determine the degree of damage to the national security, the need for continued classification, and in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences. If the agency of primary interest is other than OSTP, the matter shall be referred to that agency.

32 CFR Section 2400.10: Presumption of damage.
Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods, is presumed to cause damage to the national security.

32 CFR Section 2400.11: Duration of classification.
(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.
(b) Automatic declassification determinations under predecessor Executive Orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The originating agency shall be responsible for notifying holders of the information of such extensions.
(c) Information classified under predecessor Executive Orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of Executive Order 12356.
(d) Information classified under predecessor Executive Orders that does not bear a specific date or event for declassification shall remain classified until reviewed for declassification. The authority to extend the classification of information subject to automatic declassification under predecessor Orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the Information Security Oversight Office.

32 CFR Section 2400.12: Identification and markings.
(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:
   (1) One of the three classification levels defined in § 2400.6 of this part;
   (2) The identity of the original classification authority if other than the person whose name appears as the approving or signing official;
   (3) The agency and office of origin; and
   (4) The date or event for declassification, or the notation “Originating Agency's Determination Required.”
(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. The Director OSTP may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.
(c) Marking designations implementing the provisions of Executive Order 12356, including abbreviations, shall conform to the standards prescribed in Directive No. 1 issued by the Information Security Oversight Office.
(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of
protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor Executive Orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in § 2400.18 of this part.

32 CFR Section 2400.13: Limitations on classification.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The Director may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office. Before reclassifying any information, the Director shall consider the factors listed in § 2001.6 of Directive No. 1, which shall be addressed in the report to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after OSTP has received a request for it under the Freedom of Information Act (5 U.S.C. 552a) or the Privacy Act of 1974 (5 U.S.C. 552), or the mandatory review provisions of Executive Order 12356 (section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the Director.
SUBPART C—Derivative Classification

32 CFR Section 2400.14: Use of derivative classification.
(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult an appropriate official of the originating agency or office of origin who has the authority to declassify, downgrade or upgrade the information.
(b) Persons who apply derivative classification markings shall:
(1) Observe and respect original classification decisions; and
(2) Carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

32 CFR Section 2400.15: Classification guides.
(a) OSTP shall issue and maintain classification guides to facilitate the proper and uniform derivative classification of information. These guides shall be used to direct derivative classification.
(b) The classification guides shall be approved, in writing, by the Director or by officials having Top Secret original classification authority. Such approval constitutes an original classification decision.
(c) Each classification guide shall specify the information subject to classification in sufficient detail to permit its ready and uniform identification and categorization and shall set forth the classification level and duration in each instance. Additionally, each classification guide shall prescribe declassification instructions for each element of information in terms of (1) a period of time, (2) the occurrence of an event, or (3) a notation that the information shall not be automatically declassified without the approval of OSTP.
(d) The classification guides shall be kept current and shall be fully reviewed at least every two years. The Executive Director, OSTP shall maintain a list of all OSTP classification guides in current use.
(e) The Executive Director, OSTP shall receive and maintain the record copy of all approved classification guides and changes thereto. He will assist the originator in determining the required distribution.
(f) The Director may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers. The Director's decision to waive the requirement to issue classification guides for specific classes of documents or information will be based, at a minimum, on an evaluation of the following factors:
(1) The ability to segregate and describe the elements of information;
(2) The practicality of producing or disseminating the guide because of the nature of the information;
(3) The anticipated usage of the guide as a basis for derivative classification; and
(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

32 CFR Section 2400.16: Derivative classification markings.
(a) Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2400.12 of this part and Directive No. 1 as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide. When markings are omitted because they may reveal a confidential source or relationship not otherwise evident, as described in § 2400.12 of this part, the information may not be used as a basis for derivative classification.
(b) The authority for classification shall be shown as directed in Directive No. 1.
SUBPART D—Declassification and Downgrading

32 CFR Section 2400.17: Policy.
Declassification of information shall be given emphasis comparable to that accorded classification. Information classified pursuant to Executive Order 12356 and prior orders shall be declassified or downgraded as soon as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event which permits declassification. When information is reviewed for declassification pursuant to this regulation, that information shall be declassified unless the designated declassification authority determines that the information continues to meet the classification requirements prescribed in § 2400.9 of this part despite the passage of time. The Office of Science and Technology Policy officials shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter.

32 CFR Section 2400.18: Declassification and downgrading authority.
Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the Director, OSTP. The Executive Director, OSTP shall maintain a current listing of persons or positions receiving those delegations. If possible, these listings shall be unclassified.

32 CFR Section 2400.19: Declassification by the Director of the Information Security Oversight Office.
If the Director of the Information Security Oversight Office (ISOO) determines that information is classified in violation of Executive Order 12356, the Director, ISOO may require the information to be declassified by the agency that originated the classification. Any such decision by the Director ISOO may be appealed by the Director, OSTP to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

32 CFR Section 2400.20: Systematic review for declassification.

(a) Permanent records.
Systematic review is applicable only to those classified records, and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) Non-permanent records.
Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records
Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory review for declassification request.

(c) Office of Science and Technology Policy Responsibility.

The Director, OSTP, shall:
(1) Issue guidelines for systematic declassification review and, if applicable, for downgrading. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office and be designated to assist the Archivist in the conduct of systematic reviews;
(2) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process;
(3) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(d) Foreign Government Information.

Systematic declassification review of foreign government information shall be in accordance with guidelines issued by the Director of the Information Security Oversight Office.

(e) Special procedures.

The Office of Science and Technology Policy shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities) or intelligence sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

32 CFR Section 2400.21: Mandatory review for declassification.
(a) Except as provided in paragraph (d) of this section, all information classified under Executive Order 12356 or predecessor orders shall be subject to a review for declassification by the Office of Science and Technology Policy, if:
(1) The request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and
(2) The request is made in writing and describes the document or material containing the information with sufficient specificity to enable the Office of Science and Technology Policy to locate it with a reasonable amount of effort.
(b) Requests should be addressed to: Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.
(c) If the request does not reasonably describe the information sought to allow identification of documents containing such information, the requester shall be notified that unless additional information is provided or the request is made more specific, no further action will be taken.
(d) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically
providing advice and counsel to a President or acting on behalf of a President is exempted from the mandatory review provisions of § 2400.24(a) of this part. The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matters interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(e) Office of Science and Technology Policy officials conducting a mandatory review for declassification shall declassify information no longer requiring protection under Executive Order 12356. They shall release this information unless withholding is otherwise authorized under applicable law.

(f) Office of Science and Technology Policy responses to mandatory review requests shall be governed by the amount of search and review time required to process the request. Normally the requester shall be informed of the Office of Science and Technology Policy determination within thirty days of receipt of the original request (or within thirty days of the receipt of the required amplifying information in accordance with paragraph (c) of this section). In the event that a determination cannot be made within thirty days, the requester shall be informed of the additional time needed to process the request. However, OSTP, shall make a final determination within one year from the date of receipt of the request except in unusual circumstances.

(g) When information cannot be declassified in its entirety, OSTP will make a reasonable effort to release, consistent with other applicable law, those declassified portions of that requested information the constitute a coherent segment.

(h) If the information may not be released in whole or in part, the requester shall be given a brief statement as to the reason for denial, and notice of the right to appeal the determination in writing within sixty days of receipt of the denial to the chairperson of the Office of Science and Technology Policy Review Committee. If appealed, the requester shall be informed in writing of the appellate determination within thirty days of receipt of the appeal.

(i) When a request is received for information originated by another agency, the Executive Director, Office of Science and Technology Policy, shall:

(1) Forward the request to such agency for review together with a copy of the document containing the information requested, where practicable, and where appropriate, with the Office of Science and Technology Policy recommendation to withhold or declassify and release any of the information;
(2) Notify the requester of the referral unless the agency to which the request is referred objects to such notice on grounds that its association with the information requires protection; and
(3) Request, when appropriate, that the agency notify the Office of Science and Technology Policy of its determination.

(j) If the request requires the rendering of services for which fees may be charged under title 5 of the Independent Offices Appropriation Act, 31 U.S.C. 483a, the Executive Director, Office of Science and Technology Policy, may calculate the anticipated amount of fees to be charged.

(1) Fees for the location and reproduction of information that is the subject of a mandatory review request shall be assessed according to the following schedule:
(i) Search for records.
$5.00 per hour when the search is conducted by a clerical employee; $8.00 per hour when the search is conducted by a professional employee. No fee shall be assessed for searches of less than one hour.
(ii) Reproduction of documents.
Documents will be reproduced at a rate of $.25 per page for all copying of four pages or more. No fee shall be assessed for reproducing documents that are three pages or less, or for the first three pages of longer documents.
(2) Where it is anticipated that the fees chargeable under this section will amount to more than $25, and the requestor has not indicated in advance a willingness to pay fees as high as are anticipated, the requester shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by OSTP until a reply is received from the requester.
(3) Remittances shall be in the form either of a personal check or bank draft drawn on a bank in the United States, or a postal money order. Remittances shall be made to the Treasury of the United States and mailed to the Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.
(4) A receipt for fees paid will be given only upon request. Refund of fees paid for services actually rendered will not be made.
(5) If a requester fails to pay within thirty days for services rendered, further action on any other requests submitted by that requestor shall be suspended.
(6) The Executive Director, Office of Science and Technology Policy may waive all or part of any fee provided for in this section when it is deemed to be in either the interest of the OSTP or the general public.

The Office of Science and Technology Policy shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.
32 CFR Section 2400.23: Prohibition.
In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of Executive Order 12356 and Directive No. 1, or this regulation:
(a) The Office of Science and Technology Policy shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under Executive Order 12356.
(b) When the Office of Science and Technology Policy receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases which the originating agency determines in writing that a response under paragraph (a) of this section is required, the Office of Science and Technology Policy shall respond to the requester in accordance with that paragraph.

32 CFR Section 2400.24: Downgrading.
(a) When it will serve a useful purpose, original classification authorities may, at the time of original classification, specify that downgrading of the assigned classification will occur on a specified date or upon the occurrence of a stated event.
(b) Classified information marked for automatic downgrading is downgraded accordingly without notification to holders.
(c) Classified information not marked for automatic downgrading may be assigned a lower classification designation by the originator or by an official authorized to declassify the same information. Prompt notice of such downgrading shall be provided to known holders of the information.
SUBPART E—Safeguarding

32 CFR Section 2400.25: Access.
(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes. A personnel security clearance is an indication that the trustworthiness decision has been made. Procedures shall be established by the head of each office to prevent access to classified information before a personnel security clearance has been granted. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests with the individual who has authorized possession, knowledge, or control of the information and not with the prospective recipient. These principles are equally applicable if the prospective recipient is an organizational entity, other Federal agencies, contractors, foreign governments, and others.
(b) When access to a specific classification category is no longer required for the performance of an individual's assigned duties, the security clearance will be administratively adjusted, without prejudice to the individual, to the classification category, if any, required.
(c) The Director, Office of Science and Technology Policy may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to Executive Order 12356 or predecessor orders if:
(1) Normal management and safeguarding procedures do not limit access sufficiently;
(2) The number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information;
(3) The special access program is established in writing; and
(4) A system of accounting for the program is established and maintained.

32 CFR Section 2400.26: Access by historical researchers and former Presidential appointees.
(a) The requirement in Section 4.1(a) of Executive Order 12356 that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in paragraph (b) of this section for persons who:
(1) Are engaged in historical research projects, or
(2) Previously have occupied policy-making positions to which they were appointed by the President.
(b) Waivers under paragraph (a) of this section may be granted only if the Director, Office of Science and Technology Policy:

Page 1215
(1) Determines in writing that access is consistent with the interest of national security;
(2) Takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with Executive Order 12356;
(3) Limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee; and
(4) Has received a written agreement from the researcher or former presidential appointee that his notes can be reviewed by OSTP for a determination that no classified material is contained therein.

32 CFR Section 2400.27: Storage of classification information.
Whenever classified information is not under the personal control and observation of an authorized person, it will be guarded or stored in a locked security container approved for the storage and protection of the appropriate level of classified information as prescribed in § 2001.43 of Directive No. 1.

32 CFR Section 2400.28: Dissemination of classified information.
Heads of OSTP offices shall establish procedures consistent with this Regulation for dissemination of classified material. The originating official may prescribe specific restrictions on dissemination of classified information when necessary.
(a) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.
(b) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

32 CFR Section 2400.29: Accountability and control.
(a) Each item of Top Secret, Secret, and Confidential information is subject to control and accountability requirements.
(b) The Security Officer will serve as Top Secret Control Officer (TSCO) for the Office of Science and Technology Policy and will be responsible for the supervision of the Top Secret control program. He/she will be assisted by an Assistant Top Secret Control Officer (ATSCO) to effect the Controls prescribed herein for all Top Secret material.
(c) The TSCO shall receive, transmit, and maintain current access and accountability records for Top Secret information. The records shall show the number and distribution of all Top Secret documents, including any reproduced copies.
(d) Top Secret documents and material will be accounted for by a continuous chain of receipts.
(e) An inventory of Top Secret documents shall be made at least annually.
(f) Destruction of Top Secret documents shall be accomplished only by the TSCO or the ATSCO.
(g) Records shall be maintained to show the number and distribution of all classified documents covered by special access programs, and of all Secret and Confidential documents which are marked with special dissemination and reproduction limitations.
(h) The Security Officer will develop procedures for the accountability and control of Secret and Confidential information. These procedures shall require all Secret and Confidential material originated or received by OSTP to be controlled. Control shall be accomplished by the ATSCO.

32 CFR Section 2400.30: Reproduction of classified information.
Documents or portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be strictly observed. Copying of documents containing classified information at any level shall be minimized. Specific reproduction equipment shall be designated for the reproduction of classified information and rules for reproduction of classified information shall be posted on or near the designated equipment. Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information. All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made.

32 CFR Section 2400.31: Destruction of classified information.
(a) Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, U.S.C., which governs disposition of classified records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the Director, OSTP, as implemented by the Security Officer. These procedures and methods must provide adequate protection to prevent access by unauthorized persons and must preclude recognition or reconstruction of the classified information or material.
(b) All classified information to be destroyed will be provided to the ATSCO for disposition. Controlled documents will be provided whole so that accountability records may be corrected prior to destruction by the ATSCO.

32 CFR Section 2400.32: Transmittal of classified information.
The transmittal of classified information outside of the Office of Science and Technology Policy shall be in accordance with procedures of § 2001.44 of Directive No. 1. The Security Officer shall be responsible for resolving any questions relative to such transmittal.

32 CFR Section 2400.33: Loss or possible compromise.
(a) Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to the Security Officer. The Security Officer shall notify the Director and the agency that originated the information as soon as possible so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise.

(b) The Security Officer shall initiate an inquiry to:
   (1) Determine cause,
   (2) Place responsibility, and
   (3) Take corrective measures and appropriate administrative, disciplinary, or legal action.

(c) The Security Officer shall keep the Director advised on the details of the inquiry.
SUBPART F—Foreign Government Information
32 CFR Section 2400.34: Classification.
(a) Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a United States classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.
(b) Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that it be held in confidence must be classified because Executive Order 12356 states a presumption of damage to the national security in the event of unauthorized disclosure of such information.

32 CFR Section 2400.35: Duration of classification.
Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

32 CFR Section 2400.36: Declassification.
Officials shall respect the intent of this Regulation to protect foreign government information and confidential foreign sources.

32 CFR Section 2400.37: Mandatory review.
Except as provided in this paragraph, OSTP shall process mandatory review requests for classified records containing foreign government information in accordance with § 2400.21. The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If OSTP receives a request for mandatory review and is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

32 CFR Section 2400.38: Protection of foreign government information.
Classified foreign government information shall be protected as is prescribed by this regulation for United States classified information of a comparable level.
SUBPART G—Security Education

32 CFR Section 2400.39: Responsibility and objectives.
The OSTP Security Officer shall establish a security education program for OSTP personnel. The program shall be sufficient to familiarize all OSTP personnel with the provisions of Executive Order 12356 and Directive No. 1, and this regulation. It shall be designed to provide initial, refresher, and termination briefings to impress upon them their individual security responsibilities.
SUBPART H—Office of Science and Technology Policy Information Security Program Management

32 CFR Section 2400.40: Responsibility.
The Director, OSTP is the senior OSTP official having authority and responsibility to ensure effective and uniform compliance with and implementation of Executive Order 12356 and its implementing Directive No. 1. As such, the Director, OSTP, shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the OSTP Information Security Program. The Director, OSTP, may approve waivers or exceptions to the provisions of this regulation to the extent such action is consistent with Executive Order 12356 and Directive -No. 1.

32 CFR Section 2400.41: Office Review Committee.
The Office of Science and Technology Policy Review Committee (hereinafter referred to as the Office Review Committee) is hereby established and will be responsible for the continuing review of the administration of this Regulation with respect to the classification and declassification of information or material originated or held by the Office of Science and Technology Policy. The Office Review Committee shall be composed of the Executive Director who shall serve as chairperson, the Assistant Director for National Security & Space, and the Security Officer.

32 CFR Section 2400.42: Security Officer.
Under the general direction of the Director, the Special Assistant to the Executive Director will serve as the Security Officer and will supervise the administration of this Regulation. He/she will develop programs, in particular a Security Education Program, to insure effective compliance with and implementation of the Information Security Program. Specifically he/she also shall:
(a) Maintain a current listing by title and name of all persons who have been designated in writing to have original Top Secret, Secret, and Confidential Classification authority. Listings will be reviewed by the Director on an annual basis.
(b) Maintain the record copy of all approved OSTP classification guides.
(c) Maintain a current listing of OSTP officials designated in writing to have declassification and downgrading authority.
(d) Develop and maintain systematic review guidelines.

32 CFR Section 2400.43: Heads of offices.
The Head of each unit is responsible for the administration of this regulation within his area. These responsibilities include:
(a) Insuring that national security information is properly classified and protected;
(b) Exercising a continuing records review to reduce classified holdings through retirement, destruction, downgrading or declassification;
(c) Insuring that reproduction of classified information is kept to the absolute minimum;
(d) Issuing appropriate internal security instructions and maintaining the prescribed control and accountability records on classified information under their jurisdiction.

32 CFR Section 2400.44: Custodians.
Custodians of classified material shall be responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

32 CFR Section 2400.45: Information Security Program Review.
(a) The Director, OSTP, shall require an annual formal review of the OSTP Information Security Program to ensure compliance with the provisions of Executive Order 12356 and Directive No. 1, and this regulation.
(b) The review shall be conducted by a group of three to five persons appointed by the Director and chaired by the Executive Director. The Security Officer will provide any records and assistance required to facilitate the review.
(c) The findings and recommendations of the review will be provided to the Director for his determination.

32 CFR Section 2400.46: Suggestions or complaints.
Persons desiring to submit suggestions or complaints regarding the Office of Science and Technology Policy Information Security Program should do so in writing. This correspondence should be addressed to: Executive Director, Office of Science and Technology Policy, Executive Office of the President, Washington, DC 20506.
32 CFR PART 2700—SECURITY INFORMATION REGULATIONS

Subpart A—Introduction
  o 2700.1: References.
  o 2700.2: Purpose.
  o 2700.3: Applicability.

Subpart B—Original Classification
  o 2700.11: Basic policy.
  o 2700.12: Criteria for and level of original classification.
  o 2700.13: Duration of original classification.
  o 2700.14: Challenges to classification.

Subpart C—Derivative Classification
  o 2700.21: Definition and application.
  o 2700.22: Classification guides.

Subpart D—Declassification and Downgrading
  o 2700.31: Declassification authority.
  o 2700.32: Declassification general.
  o 2700.33: Mandatory review for declassification.
  o 2700.34: Downgrading authority.

Subpart E—Safeguarding
  o 2700.41: General restrictions on access.
  o 2700.42: Responsibility for safeguarding classified information.
  o 2700.43: Reproduction controls.
  o 2700.44: Administrative sanctions.

Subpart F—Implementation and Review
  o 2700.51: Information Security Oversight Committee.
  o 2700.52: Classified Review Committee.

Authority:

Source:
44 FR 51574, Sept. 4, 1979, unless otherwise noted. Correctly designated at 44 FR 51990, Sept. 6, 1979.
SUBPART A—Introduction

32 CFR Section 2700.1: References.

32 CFR Section 2700.2: Purpose.
The purpose of this Regulation is to ensure, consistent with the authorities listed in § 2700.1, that national security information originated and/or held by the Office for Micronesian Status Negotiations (OMSN), which includes the Status Liaison Office, Saipan, Northern Mariana Islands (SLNO), is protected. To ensure that such information is protected, but only to the extent and for such period as is necessary, this regulation identifies the information to be protected and prescribes certain classification, declassification and safeguarding procedures to be followed.

32 CFR Section 2700.3: Applicability.
This Regulation supplements E.O. 12065 within OMSN with regard to National Security Information. In consonance with the authorities listed in § 2700.1, it establishes general policies and certain procedures for the classification, declassification and safeguarding of information which is owned by, is produced for or by, or is under the control of OMSN.
SUBPART B—Original Classification
32 CFR Section 2700.11: Basic policy.

(a) General.

It is the policy of OMSN to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security.

(b) Safeguarding national security information.

Within the Federal Government there is some information which because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our nation.

(c) Balancing test.

To balance the public's interest in access to government information with the need to protect certain national security information from disclosure, these regulations indentify the information to be protected, prescribe classification, downgrading, declassification, and safeguarding procedures to be followed, and establish education, monitoring and sanctioning systems to insure their effectiveness. When questions arise as whether the need to protect information may be outweighed by the public interest in disclosure of the information, they shall be referred to OMSN pursuant to § 2700.32(b) for a determination whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

32 CFR Section 2700.12: Criteria for and level of original classification.

(a) General Policy.

Documents or other material are to be classified only when protecting the national security requires that the information they contain be withheld from public disclosure. Information may not be classified to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization or agency, or to restrain competition. No material may be classified to limit dissemination, or to prevent or delay public release, unless its classification is consistent with E.O. 12065.

(b) Criteria.

To be eligible for classification, information must meet two requirements:
(1) First, it must deal with one of the criteria set forth in section 1-301 of E.O. 12065;
(2) Second, the President’s Personal Representative for Micronesian Status Negotiations or his delegate who has original classification authority must determine that unauthorized disclosure of the information or material can reasonably be expected to cause at least identifiable harm to the national security.

(c) Classification designations.

Only three designations of classification are authorized—“Top Secret,” “Secret,” “Confidential.” No other classification designation is authorized or shall have force.

(d) Unnecessary classification, and classification at a level higher than is necessary, shall be avoided. If there is reasonable doubt as to which designation in section 1-1 of E.O. 12065 is appropriate, or whether information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

32 CFR Section 2700.13: Duration of original classification.

(a) Information or material which is classified after December 1, 1978, shall be marked at the time of classification with the date or event for declassification or a date for review for declassification. This date or event shall be as early as national security permits and shall be no more than six years after original classification except as provided in paragraph (b) of this section.

(b) Only the President’s Personal Representative for Micronesian Status Negotiations may authorize a classification period exceeding six years. Originally classified information that is so designated shall be identified with the authority and reason for extension. This authority shall be used sparingly. In those cases where extension of classification is warranted, a declassification date or event, or a date for review shall be set. This date or event shall be early as national security permits and shall be no more than twenty years after original classification except that for foreign information the date or event may be up to thirty years after original classification.

32 CFR Section 2700.14: Challenges to classification.

If holders of classified information believe the information is improperly or unnecessarily classified, or that original classification has been extended for too long a period, they should discuss the matter with their immediate superiors or the classifier of the information. If these discussions do not satisfy the concerns of the challenger, the matter should be brought to the attention of the chairman of the OMSN Information Security Oversight Committee, established pursuant to § 2700.51. Action on such challenges shall be taken within 30 days from date of receipt and the challenger shall be notified of the results. When requested, anonymity of the challenger shall be preserved.
SUBPART C—Derivative Classification

32 CFR Section 2700.21: Definition and application.
Derivative classification is the act of assigning a level of classification to information which is determined to be the same in substance as information which is currently classified. Thus, derivative classification may be accomplished by any person cleared for access to that level of information, regardless of whether the person has original classification authority at that level.

32 CFR Section 2700.22: Classification guides.
OMSN shall issue classification guides pursuant to section 2-2 of E.O. 12065. These guides, which shall be used to direct derivative classification, shall identify the information to be protected in specific and uniform terms so that the information involved can be readily identified. The classification guides shall be approved in writing by the President's Personal Representative for Micronesian Status Negotiations. Such approval constitutes an original classification decision. The classification guides shall be kept current and shall be reviewed at least every two years.
SUBPART D—Declassification and Downgrading

32 CFR Section 2700.31: Declassification authority.
The Director, OMSN, is authorized to declassify OMSN originated documents after consultation with the appropriate OMSN staff members.

32 CFR Section 2700.32: Declassification general.
Declassification of classified information shall be given emphasis comparable to that accorded to classification. The determination to declassify information shall not be made on the basis of the level of classification assigned, but on the loss of the sensitivity of the information with the passage of time, and with due regard for the public interest in access to official information. At the time of review, any determination not to declassify shall be based on a determination that despite the passage of time since classification, release of information reasonably could still be expected to cause at least identifiable damage to the national security.

32 CFR Section 2700.33: Mandatory review for declassification.

(a) General.
All information classified under the Order or prior orders, except as provided for in section 3-503 of E.O. 12065 shall be subject to review for declassification upon request of a member of the public, a government employee, or an agency.

(b) Receipt.
(1) Requests for mandatory review for declassification under section 3-501 of E.O. 12065 must be in writing and should be addressed to: Office for Micronesian Status Negotiations, ATTN: Security Officer (Mandatory Review Request), Room 3356, Department of the Interior, Washington, DC 20240.
(2) The requestor shall be informed of the date of receipt of the request at OMSN. This date will be the basis for the time limits specified in paragraph (c) of this section.
(3) If the request does not reasonably describe the information sought, the requestor shall be notified that, unless additional information is provided or the request is made more specific, no further action will be taken.
(4) Subject to paragraph (b)(7) of this section, if the information requested is in the custody of and under the exclusive declassification authority of OMSN, OMSN shall determine whether the information or any reasonably segregable portion of it no longer requires protection. If so, OMSN shall promptly make such information available to the requester, unless withholding it is otherwise warranted under applicable law. If the information may not be released, in whole or in part, OMSN shall give the requester a brief statement of the reasons, a notice of the right to appeal the determination to the agency review committee, and notice that such an appeal must be filed with the review committee within 60 days.
(5) When OMSN receives a request for information in a document which is in its custody, but which was classified by another agency, it shall refer the request to the appropriate agency for review, together with a copy of the document containing the information requested, where practicable. OMSN shall also notify the requester of the referral, unless the association of the reviewing agency with the information requires protection. The reviewing agency shall review a document in coordination with any other agency involved with the classification or having a direct interest in the subject matter. The reviewing agency shall respond directly to the requester in accordance with the pertinent procedures described above and, if requested, shall notify OMSN of its determination.

(6) Requests for declassification of classified documents originated by OMSN or another agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C 2107 or 2107 Note, shall be referred by the Archivist to the agency of origin for processing and for direct response to the requests. The Archivist will inform requesters of such referrals.

(7) In the case of requests for documents containing foreign government information, OMSN, if it is also the agency which initially received the foreign government information, shall determine whether the foreign government information in the document may be declassified and released in accordance with agency policies or guidelines, consulting with other agencies of subject matter interest as necessary. If OMSN is not the agency which received the foreign government information, it shall refer the request to the latter agency, which shall take action on the request. In those cases where available agency policies or guidelines do not apply, consultation with the foreign originator through appropriate channels may be advisable prior to final action on the request.

(8) If any agency makes a request on behalf of a member of the public, the request shall be considered as a request by that member of the public and handled accordingly.

(c) Review.

(1) Within sixty days from its receipt, OMSN shall inform the requestor of the determination of the mandatory review for declassification.

(2) If the determination is to withhold some or all of the material requested, the requestor may appeal the determination. The requestor shall be informed that an appeal must be made in writing within sixty days of receipt of the denial and should be addressed to the chairperson of the OMSN Classification Review Committee established pursuant to § 2700.52.

(3) No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act (5 U.S.C. 552) or under section 3-5 of E.O. 12065, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable.

(4) The requestor shall be informed of the appellate determination within thirty days of receipt of the appeal.
(5) In considering requests for mandatory review, OMSN may decline to review again any request for material which has been recently reviewed and denied, except insofar as the request constitutes an appeal under paragraph (f) of this section.

(d) Processing of Requests.

The processing of requests by OMSN shall be as follows:
(1) The Security Officer or his designee shall record the request, and arrange for search and review of the documents. The documents will be reviewed for declassification in accordance with these regulations or any applicable guidelines. If the documents remain classified and are not to be released, in whole or in part, the reviewing office will also prepare a letter informing the requester as described in paragraph (b)(4) of this section. The letter to the requester shall be signed by the President's Personal Representative for Micronesian Status Negotiations, his Deputy or the Status Liaison Officer. The Security Officer or his designee shall record disposition of the case and forward the letter of denial to the requester.
(2) If any request requires obtaining the views of other agencies, the receiving office shall arrange coordination of review with such other agencies.
(3) When all documents involved in the request are declassified and released, the receiving office will send a release statement, to the requester, and shall inform the requester of any fees due before releasing documents.
(4) In the case of documents of agency origin requested by a Presidential Library on behalf of a member of the public, if there is a partial denial, the letter will advise the requester as described in paragraph (b)(4) of this section, but the requester will be referred to the Archivist for copies of the released document, with portions excised. The receiving office will transmit such documents, with portions marked to be excised, to Archives which will transmit them with portions excised to the Presidential Library for its records and for use in the case of further similar requests.
(5) The Security Officer or his designee shall also coordinate requests from other agencies seeking the views of OMSN as to declassification of documents originated by such other agencies but involving information of primary subject matter interest to OMSN. The Security Officer or his designee will transmit the documents to the reviewing individual for a determination as to declassification and will coordinate the reply of OMSN to the requesting agency.

(e) Appeals.

(1) The President's Personal Representative for Micronesian Status Negotiations shall receive appeals for denial of documents by OMSN. Such appeals shall be addressed to President's Personal Representative for Micronesian Status Negotiations, Suite 3356, Interior Department Building, Washington, DC 20240. The appeal must be received in OMSN within 60 days of the date of the original denial letter or the final release of documents, whichever is later.
(2) Appeals shall be decided within 30 days of their receipt.

Page 1230
(f) Fees.

(1) Fees for the location and reproduction of information which is the subject of a mandatory review request shall be assessed according to the following schedule:

(i) Search for records: $5.00 per hour when the search is conducted by a clerical employee; $8.00 per hour when the search is conducted by a professional employee. No fee shall be assessed for searches of less than one hour.

(ii) Reproduction of documents: Documents will be reproduced at a rate of $.25 per page for all copying of four pages or more. No fee shall be assessed for reproducing documents which are three pages or less, or for the first three pages of longer documents.

(2) Where it is anticipated that the fees chargeable under this section will amount to more than $25.00, and the requestor has not indicated in advance a willingness to pay fees as high as are anticipated, the requestor shall be promptly notified of the amount of the anticipated fee or such portion thereof as can readily be estimated. In instances where the estimated fees will greatly exceed $25.00, an advance deposit may be required. Dispatch of such a notice or request shall suspend the running of the period for response by OMSN until a reply is received from the requestor.

(3) Remittance shall be in the form either of a personal check or bank draft on a bank in the United States, or a postal money order. Remittance shall be made payable to Treasurer of the United States and mailed to the address noted in paragraph (b)(1) of this section.

(4) A receipt for fees paid will be provided only upon request. Refund of fees for services actually rendered will not be made.

(5) OMSN may waive all or part of any fee provided for in this section when it is deemed to be in either the interest of OMSN or of the general public.

32 CFR Section 2700.34: Downgrading authority.
The Security Officer, OMSN is authorized to downgrade OMSN originated documents after consultation with the staff member who is charged with functional responsibility for the subject matter under question.
SUBPART E—Safeguarding

32 CFR Section 2700.41: General restrictions on access.

(a) Determination of need-to-know.

Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance, except as provided in section 4-3 of E.O. 12065, that access is essential to the accomplishment of official Government duties or contractual obligations.

(b) Determination of Trustworthiness.

A person is eligible for access to classified information only after a showing of trustworthiness as determined by the President's Personal Representative for Micronesian Status Negotiations based upon appropriate investigations in accordance with applicable standards and criteria.

32 CFR Section 2700.42: Responsibility for safeguarding classified information.

(a) General Policy.

The specific responsibility for the maintenance of the security of classified information rest with each person having knowledge or physical custody thereof, no matter how obtained. The ultimate responsibility for safeguarding classified information rests on each supervisor to the same degree that supervisor is charged with functional responsibility.

(b) Security and Top Secret Control Officers.

The Director, OMSN, and the Status Liaison Officer, Saipan, are assigned specific security responsibilities as Security Officer and Top Secret Control Officer.

(c) Handling.

All documents bearing the terms “Top Secret,” “Secret” and “Confidential” shall be delivered to the Top Secret Control Officer or his designee immediately upon receipt. All potential recipients of such documents shall be advised of the names of such designees and updated information as necessary. In the event that the Top Secret Control Officer or his designees are not available to receive such documents, they shall be turned over to the office supervisor and secured, unopened, in a designated combination safe located in OMSN or SLNO, as appropriate until the Top Secret Control Officer is available. All materials not immediately deliverable to the Top Secret Control Officer shall be delivered at the earliest opportunity. Under no circumstances shall classified material that cannot
be delivered to the Top Secret Control Officer be stored other than in the designated safe.

(d) Storage.

All classified documents shall be stored in the designated combination safe or safes located in OMSN or SLNO as appropriate. The combination shall be changed as required by ISOO Directive No. 1, section IV F (5)(a). The combinations shall be known only to the Security Officer and his designees with the appropriate security clearance.

(e) Security Education Program.

The Security Officer shall establish a program of briefings to familiarize personnel with the provisions of E.O. 12065 and implementing directives. Such briefings shall be held once per year, or more frequently. Before any new or newly assigned employee enters on duty, he shall be given instruction in sufficient detail in security procedures and practices to inform him of his responsibilities arising from his access to classified data.

(f) Access by Historical Researchers and Former Presidential Appointees.

In keeping with provisions 4-301 and 4-302 of E.O. 12065, the President's Personal Representative for Micronesian Status Negotiations shall designate appropriate officials to determine, prior to granting access to classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know.

32 CFR Section 2700.43: Reproduction controls. OMSN and SLNO shall maintain records to show the number and distribution of all OMSN originated classified documents. Reproduction of classified material shall take place only in accordance with section 4-4 of E.O. 12065 and any limitations imposed by the originator. Should copies be made, they are subject to the same controls as the original document. Records showing the number of distribution of copies shall be maintained by the Office Supervisor and the log stored with the original documents. These measures shall not restrict reproduction for the purposes of mandatory review.

32 CFR Section 2700.44: Administrative sanctions. Officers and employees of the United States Government assigned to OMSN shall be subject to appropriate administrative sanctions if they knowingly and willingly commit a violation under section 5-5 of E.O. 12065. These sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law or the applicable regulations of the agency from which they are assigned to OMSN.
SUBPART F—Implementation and Review

The OMSN Information Security Oversight Committee shall be chaired by the Security Officer, OMSN. The Committee shall be responsible for acting on all suggestions and complaints concerning the administration of the OMSN information security program. The chairperson shall also be responsible for conducting an active oversight program to ensure effective implementation of E.O. 12065.

32 CFR Section 2700.52: Classified Review Committee.
The OMSN Classification Review Committee shall be chaired by the President's Personal Representative for Micronesian Status Negotiations. The Committee shall decide appeals from denials of declassification requests submitted pursuant to section 3-5 of E.O. 12065. The Committee shall consist of the President's Personal Representative, Department of Defense/Legal Advisor and Political/Economic Advisor.
32 CFR CHAPTER XXVIII—OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES

32 CFR PART 2800—SECURITY PROCEDURES

- 2800.1: Purpose.
- 2800.2: Guiding directives.
- 2800.3: Policy.
- 2800.4: General information.
- 2800.5: Policies.
- 2800.6: Delegation of classification and declassification authority.
- 2800.7: Designation of chairperson for Ad Hoc Committees.

- Attachment 1 to Part 2800—Employment Agreement & Indocritnation Statement
- Attachment 2 to Part 2800—Security Termination Statement
- Attachment 3 to Part 2800—Sample

Authority:

Source:
44 FR 66591, Nov. 20, 1979, unless otherwise noted.
32 CFR Section 2800.1: Purpose.
To establish procedures and provide guidance for the security of classified information and material within the Office of the Vice President.

32 CFR Section 2800.2: Guiding directives.

32 CFR Section 2800.3: Policy.
The classification, declassification, safeguarding and handling of classified information within the Office of the Vice President will comply with the letter and spirit of those directives listed in § 2800.2. All personnel of the Office of the Vice President are responsible individually for complying with the provisions of these regulations in all respects. The provisions of these regulations applicable to all personnel assigned or detailed to the Office of the Vice President.

32 CFR Section 2800.4: General information.
(a) Staff Security Officer/Top Secret Control Officer.
A Vice Presidential Staff Security Officer and Assistant Staff Security Officer will be assigned to perform the duties as outlined in these regulations. They will normally be on the staff of the Assistant to the Vice President for National Security Affairs. The Staff Security Officer and Assistant Staff Security Officer will serve as Top Secret Control Officer and Assistant Top Secret Control Officer and custodians of classified material for the Office of the Vice President respectively, and will be responsible for the overall supervision of the Top Secret Control program. They will maintain positive control over the movement of all Top Secret material under their jurisdiction.

(b) Custodian, Office of the Assistant to the Vice President for Congressional Relations.
The Assistant to the Vice President for Congressional Relations, Office of the President of the Senate, will be designated as Custodian of classified material for that office. He will be responsible for compliance with the instructions contained herein. In this capacity, he will be charged with safeguarding classified material necessary to the operation of the office.

(c) National Security Classifications.
Classifications of National Security Information are defined in Executive Order 12065, sections 1-102 through 1-104.

(d) Prohibited Markings.
(1) The caveats “FOR OFFICIAL USE ONLY” and “ADMINISTRATIVELY RESTRICTED” are used within the Office of the Vice President to designate certain unclassified information which requires control. These caveats will under no circumstances be applied to information which qualifies as classified information. Further, neither they nor other terms will be used in conjunction with the prescribed security classifications of CONFIDENTIAL, SECRET and TOP SECRET.

(2) Unclassified information bearing either of the foregoing administrative designations cannot be protected from release under the national security exemption of the Freedom of Information Act (although other exemptions may be available).

(e) Security Clearances.

No person shall be given access to classified information or material unless a favorable background investigation has been completed determining that the individual is trustworthy and that access is necessary for the performance of official duties.

(1) Security Clearance Procedures.

(i) The Counsel to the Vice President will:

(A) Be responsible for the processing of full field investigations for personnel assigned to the Vice President's staff. Department of Defense detailees are processed by the Defense Investigative Service.
(B) Inform the Staff Security Office of individuals whose full field investigations have been satisfactorily completed and approved and of any subsequent changes.
(C) Notify the Staff Security Office as soon as he/she is aware that a staff member is planning to terminate his/her employment.

(ii) The Staff Security Office will provide newly cleared persons with a security orientation briefing covering policy and procedures for handling classified information and material. After the briefing individuals will sign a Statement of Understanding of Security Procedures (Attachment 1). This statement will be kept on file by the Staff Security Office.

(iii) There is no such thing as an “Interim Security Clearance” for persons employed by or detailed to the Office of the Vice President. Under no circumstances will uncleared persons be given access to classified material. Access to classified material will be denied until the individual has had a satisfactorily completed background investigation, has received the security orientation briefing and signed the Statement of Understanding of Security Procedures.

(iv) The Staff Security Office, as part of an individual's departure debriefing, will remind them of their continuing responsibilities to protect classified information to which they have had access during the performance of their official duties. After being debriefed, the individual will sign a Security Termination Statement acknowledging his responsibilities (Attachment 2).

(2) Satisfactory completion of a background investigation does not in itself grant an individual access to classified information. Individual clearances for access to
classified information or material will be controlled by the Staff Security Office and certified in writing on an individual basis.

(f) Access to Classified Material.

Each member of the staff who has custody or possession of classified information is responsible for providing the required degree of protection from unauthorized disclosure at all times.

(1) Classified information and material will only be disclosed to an individual after it has been determined that the individual possesses the required clearance and has a valid “need to know.” Persons releasing the information shall be responsible in every case for determining the recipient’s eligibility for access.

(2) Access to Sensitive Compartmented Intelligence Information will be controlled by the Assistant to the Vice President for National Security Affairs.

(g) Custody and safekeeping of Classified Material.

(1) Classified material addressed to the Office of the Vice President will normally be delivered to and receipted for by the Staff Security Office where it will be entered into the classified material control system.

(i) Staff members receiving classified material from any source by any means will personally deliver such material to the Staff Security Office for appropriate entry into the classified control system.

(ii) Conversely, members of the staff desiring to transmit classified material will deliver the material to the Staff Security Office for handling in accordance with paragraph (h)(5) of this section.

(2) Storage of Classified Material.

(i) Classified material will be stored only in accordance with the provisions of ISOO Directive No. 1, paragraph IV-F-1 through 4.

(ii) Filing of unclassified material in security containers is prohibited except where the unclassified material is an integral part of a file which contains classified material. If extenuating circumstances necessitate the use of a security container for storing only unclassified material, the container will be marked with a sign stating “This container is not used to store classified material” or “Do not store classified material in this container.”

(3) Record of safe locations.

The Staff Security Office will assign numbers to all security containers used to store classified material in the Office of the Vice President. A record of safe numbers, locations and date of last combination change will be maintained in the Staff Security Office.

(4) Changing of lock combinations.

Combinations of security containers will be changed by the Staff Security Office or the Secret Service. This service may be requested by contacting the Staff Security Office. Combinations will be changed in accordance with the provisions of ISOO Directive No. 1, paragraph IV-F-5.

(5) Records of combinations.
Records of combinations shall be maintained by the Staff Security Office. Whenever a combination is changed, the new combination and other required information will be recorded on GSA Optional Form 63. The sealed envelope will then be delivered to the Staff Security Office for retention in the vault safe.

(6) Custodians.
Each container used for storage of classified material within the Office of the Vice President will have assigned a primary and alternate custodian. Responsibility for security of these containers shall rest with those persons, and their names shall be affixed on the outside of the top drawer of each container positioned so as to be readily discernible. Optional Form 63 shall be used for this purpose.

(h) Handling of Classified Material

(1) Use of cover sheets.
A separate cover sheet indicating the classification of the material will be fastened to the top page of cover of each CONFIDENTIAL, SECRET or TOP SECRET document.

(2) Unattended documents.
Classified material will be under the direct supervision of a person with an appropriate security clearance and a verified need-to-know at all times when in use. Special care will be taken to insure that classified material is not left unsecured or unattended in an office.

(3) Working papers.
Working papers are documents, including drafts, photographs, etc., created to assist in the formulation and preparation of finished papers. Working papers containing classified information will be marked with the appropriate classification and provided the same degree of protection as that given to other documents of an equal category of classification.

(4) Communications security.
Classified information shall not be discussed over any voice communications device except as authorized over approved secure communications circuits. This restriction also applies to electrical transmission of classified material via any unsecure circuitry involving teletypes, DEX equipment or other systems of a like nature. Appropriate secure facilities for the discussion or transmittal of classified material may be arranged by contacting the Staff Security Office.

(5) Transmittal of Classified Material
—(i) Outside the Office of the Vice President and the White House Complex.
The Staff Security Office is responsible for transmitting or transferring all classified material outside the Office of the Vice President and the White House Complex in accordance with the provisions of ISOO Directive No. 1, paragraphs I, G and H.
(ii) Within the Office of the Vice President and the White House Complex.
Transfer or movement of classified material will be accomplished only by properly cleared persons handcarrying the material to the recipient. The material
shall be carried in an envelope marked with the appropriate classification. Use of see through messenger envelopes is not authorized.

Recipients will sign a receipt (GSA Optional Form 112) for all material classified SECRET and TOP SECRET. Whenever TOP SECRET material is transferred, the Staff Security Office will be notified in order to maintain accurate accountability of the material. Classified material will never be delivered to an uncleared person, left in an unoccupied office, or sent through unclassified mail delivery/distribution systems.

(iii) Staff members requiring the use of classified material at conferences or meetings held outside the Washington, DC Metropolitan area and who intend to use commercial transportation shall provide the material to the Staff Security Office far enough in advance to assure that the material will be available on or before the date needed. This requirement does not apply when utilizing government/military transportation. In this case, material may be handcarried. The Staff Security Office will brief each staff member prior to departure concerning security requirements or arrangements needed to safeguard the material while away from his office. For meetings or conferences within the Washington, DC Metropolitan area, members may handcarry classified material. Use of classified material during a conference or meeting requires increased awareness and precautionary handling to avoid security violations and/or compromises. Staff members using classified material during a meeting or conference are responsible for ensuring that the material is properly protected at all times, and that personnel present possess appropriate clearances for the material being presented.

(iv) Visits to foreign countries.

Special precautions must be taken when visiting foreign countries to ensure classified material is protected at all times. For all visits to foreign countries a member of the staff will be appointed as custodian for all classified material required for the success of the mission. This individual will be the holder of a diplomatic passport which exempts him from customs inspections. Individual so designated will coordinate with United States embassy personnel in the country to be visited for securing of classified material within the embassy compound or other appropriate secure area during the course of the visit.

(6) Preparation and marking of Classified Material.

All classified material originating within the office of the Vice President will be prepared and marked by properly authorized and cleared personnel in accordance with ISOO Directive No. 1, paragraphs I, G, and H. A sample letter is attached for your guidance (Attachment 3). Derivative information will be prepared and classified in accordance with ISOO Directive No. 1, paragraphs II A through C. Questions concerning procedures should be directed to the Staff Security Office.

(7) Reproduction of Classified Material.

(i) Reproduction of classified material will be accomplished only by properly cleared persons.

(ii) Reproduction of TOP SECRET material will be accomplished only by a member of the Staff Security Office or a designated representative of that office.
(iii) Accountability of reproduced classified material will be maintained by informing the Staff Security Office of the reproduction of SECRET and TOP SECRET material, the number of copies reproduced and their disposition.
(iv) Reproduction machines can retain the imagery of material passed through them. Therefore, to avoid inadvertent disclosure of classified information through subsequent use of machines, staff members will always run machines through four cycles (four blank pages) after the last page of the classified material has been reproduced. These pages will be destroyed in the same manner as classified material.

(8) Destruction of Classified Material.
(i) SECRET and TOP SECRET material will be given to the Staff Security Office for destruction to insure destruction is properly recorded and destroyed material is removed from the classified control system.
(ii) CONFIDENTIAL material may be destroyed in the holder's office by tearing lengthwise and placing in a “Burn Bag” specifically designated for classified material.
(iii) Classified waste material will be separated from other office waste material and placed in “Burn Bags.” Classified waste material includes working papers, notes, drafts of classified correspondence, carbon paper, typewriter ribbons and any other material containing information requiring destruction. “Burn Bags” will be collected daily by a member of the White House Executive Protective Service who will then dispose of the bags in a secure facility.
(iv) Typewriter ribbons.
Classified material can be reproduced from imprints on used typewriter ribbons. Therefore, ribbons which are used in the preparation of classified material must be safeguarded accordingly, i.e., they will be stored in a safe at the close of business, destroyed as classified waste when no longer serviceable, etc.

(9) Inventories.
The Staff Security Office will conduct inventories of all TOP SECRET material charged to the Office of the Vice President at least annually to determine the adequacy of control procedures and insure accountability.

(i) Loss or compromise.
Any person who has knowledge of loss of possible compromise of classified information shall promptly report the circumstances to the Staff Security Office for appropriate action in accordance with ISOO Directive No. 1, paragraph IV, H.

(j) Penalties.
Any individual breach of security may warrant penalties up to and including the separation of the individual from his employment or criminal prosecution.

(k) Special access.
Special access authority is required for release of Sensitive Compartmented Intelligence Information. The names of personnel cleared for access to this category of information are on file in the Staff Security Office.

32 CFR Section 2800.5: Policies.

(a) Basic policy.

Except as provided in the Atomic Energy Act of 1943, as amended, Executive Order 12065, as implemented by ISOO Directive No. 1, provides the only basis for classifying information. It is the policy of this office to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

(b) Duration of classification.

Classification shall not be continued longer than necessary for the protection of national security. Each decision to classify requires a simultaneous determination of the duration such classification must remain in effect. For further guidance, refer to sections 1-401 and 1-402, E.O. 12065.

(c) Declassification.

Declassification of information shall be given emphasis comparable to that accorded to classification. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or upon the occurrence of a declassification event. For further guidance, refer to sections 3-102, 3-103 and 3-104 of E.O. 12065.

(d) Systematic review for declassification.

Systematic review for declassification will be in accordance with sections 3-204, 3-401 and 3-503 of E.O. 12065.

(e) Mandatory review requests.

Requests from a member of the public, a government employee, or an agency, to declassify and release information will be acted upon within 60 days provided the request reasonably identifies the information. After review, the information or any reasonably segregable portion thereof that no longer requires protection, shall be declassified and released, except as provided in section 3-503, E.O. 12065, unless withholding is otherwise warranted under applicable law.

(f) Classification guides.
The Chief Counsel, National Security Council, has determined that, in view of the limited amount of material originally classified by this office, the preparation and publication of classification guides is not required.

(g) Access to Classified Information by historical researchers and former Presidential appointees.

Access may be granted under the provisions of section 4-3 of E.O. 12065; however, access is permissive and not mandatory.

32 CFR Section 2800.6: Delegation of classification and declassification authority.

Pursuant to the provisions of sections 1-201 and 3-103 of E.O. 12065 of June 28, 1978, the following officials within the Office of the Vice President, are designated to originally classify and declassify information as “SECRET” and/or “CONFIDENTIAL”:
(a) Chief of Staff to the Vice President.
(b) Counsel to the Vice President.
(c) Executive Assistant to the Vice President.
(d) Assistant to the Vice President for National Security Affairs.
(e) Assistant to the Vice President for Issues Development and Domestic Policy.
(f) Additionally, the following individuals are designated to declassify “SECRET” and/or “CONFIDENTIAL” information in accordance with section 3-103 of E.O. 12065:
(i) Staff Security Officer/Top Secret Control Officer.
(ii) Assistant Staff Security Officer/Assistant Top Secret Control Officer.

32 CFR Section 2800.7: Designation of chairperson for Ad Hoc Committees.

The Counsel to the Vice President is designated as the responsible official to chair Ad Hoc Committees as necessary to act on all suggestions and complaints with respect to the administration of the information security program.
NON-LEGISLATIVE AND OTHER AGENCY RULES

Non-Legislative Rules Relevant to U.S. Intelligence Law
Table of Contents

  - C1.1. Applicability and Scope
  - C1.2. Scope
  - C1.3. Interpretation
  - C1.4. Exceptions to Policy
  - C1.5. Amendment
  - C2.1. Applicability and Scope
  - C2.2. Explanation of Undefined Terms
  - C2.3. Types of Information that May be Collected About United States Persons
  - C2.4. General Criteria Governing the Means Used to Collect Information About United States Persons
  - C2.5. Special Limitation on the Collection of Foreign Intelligence Within the United States
  - C3.1. Applicability
  - C3.2. Explanation of Undefined Terms
  - C3.3. Criteria for Retention
  - C3.4. Access and Retention
• Chapter 4: Procedure 4. Dissemination of Information About United States Persons
  o C4.1. Applicability and Scope
  o C4.2. Criteria for Dissemination
  o C4.3. Other Dissemination
• Chapter 5: Procedure 5. Electronic Surveillance
  o C5.1. Part 1. Electronic Surveillance in the United States for Intelligence Purposes
  o C5.2. Part 2. Electronic Surveillance Outside the United States for Intelligence Purposes
  o C5.3. Part 3. Signals Intelligence Activities
  o C5.4. Part 4. Technical Surveillance Countermeasures
  o C5.5. Part 5. Developing, Testing and Calibration of Electronic Equipment
  o C5.6. Part 6. Training of Personnel in the Operation and Use of Electronic Communications and Surveillance Equipment
  o C5.7. Part 7. Conduct of Vulnerability and Hearability Surveys
• Chapter 6: Procedure 6. Concealed Monitoring
  o C6.1. Applicability and Scope
  o C6.2. Explanation of Undefined Terms
  o C6.3. Procedures
• Chapter 7: Procedure 7. Physical Searches
  o C7.1. Applicability and Scope
  o C7.2. Explanation of Undefined Terms
  o C7.3. Procedures
• Chapter 8: Procedure 8. Searches and Examination of Mail
  o C8.1. Applicability
  o C8.2. Explanation of Undefined Terms
  o C8.3. Procedures
• Chapter 9: Procedure 9. Physical Surveillance
  o C9.1. Applicability
  o C9.2. Explanation of Undefined Terms
  o C9.3. Procedures
• Chapter 10: Procedure 10. Undisclosed Participation in Organizations
  o C10.1. Applicability
  o C10.2. Explanation of Undefined Terms
  o C10.3. Procedures for Undisclosed Participation
  o C10.4. Disclosure Requirement
• Chapter 11: Procedure 11. Contracting for Goods and Services
  o C11.1. Applicability
  o C11.2. Procedures
  o C11.3. Effect of Noncompliance
• Chapter 12: Procedure 12. Provision of Assistance to Law Enforcement Authorities
  o C12.1. Applicability
• Chapter 13: Procedure 13. Experimentation on Human Subjects for Intelligence Purposes
  o C13.1. Applicability
  o C13.2. Explanation of Undefined Terms
  o C13.3. Procedures
• Chapter 14: Procedure 14. Employee Conduct
  o C14.1. Applicability
  o C14.2. Procedures
• Chapter 15: Procedure 15. Identifying, Investigating, and Reporting Questionable Activities
  o C15.1. Applicability
  o C15.2. Explanation of Undefined Terms
  o C15.3. Procedures
REFERENCES

- Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978"
- Chapters 105 and 119 of title 18, United States Code
- Public Law 73-416, "Communications Act of 1934," Section 605
- Sections 801-840 of title 10, United States Code, "Uniform Code of Military Justice"
- Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979
- DoD Directive 5000.11, "Data Elements and Data Codes Standardization Program," December 7, 1964

Page 1248
DL1. DEFINITIONS

DL1.1.1. Administrative Purposes
Information is collected for "administrative purposes" when it is necessary for the administration of the component concerned, but is not collected directly in performance of the intelligence activities assigned such component. Examples include information relating to the past performance of potential contractors; information to enable such components to discharge their public affairs and legislative duties, including the maintenance of correspondence files; the maintenance of employee personnel and training records; and training materials or documents produced at training facilities.

DL1.1.2. Available Publicly
Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

DL1.1.3. Communications Security
Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such telecommunications.

DL1.1.4. Consent
The agreement by a person or organization to permit DoD intelligence components to take particular actions that affect the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure. Consent may be implied if adequate notice is provided that a particular action (such as entering a building) carries with it the presumption of consent to an accompanying action (such as search of briefcases). (Questions regarding what is adequate notice in particular circumstances should be referred to the legal office responsible for advising the DoD intelligence component concerned.)

DL1.1.5. Counterintelligence
Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.
DL1.1.6. Counterintelligence Investigation
Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

DL1.1.7. DoD Component
Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

DL1.1.8. DoD Intelligence Components
Include the following organizations:
- DL1.1.8.2. The Defense Intelligence Agency.
- DL1.1.8.3. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- DL1.1.8.4. The Assistant Chief of Staff for Intelligence, Army General Staff.
- DL1.1.8.5. The Office of Naval Intelligence.
- DL1.1.8.6. The Assistant Chief of Staff, Intelligence, U.S. Air Force.
- DL1.1.8.7. The Army Intelligence and Security Command.
- DL1.1.8.8. The Naval Intelligence Command.
- DL1.1.8.10. The Director of Intelligence, U.S. Marine Corps.
- DL1.1.8.11. The Air Force Intelligence Service.
- DL1.1.8.15. The 650th Military Intelligence Group, SHAPE.
- DL1.1.8.16. Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

DL1.1.9. Electronic Surveillance
Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio
direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b))).

**DL1.1.10. Employee**
A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency.

**DL1.1.11. Foreign Intelligence**
Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

**DL1.1.12. Foreign Power**
Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

**DL1.1.13. Intelligence Activities**
Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a)).

**DL1.1.14. Intelligence Community and an Agency of Or Within the Intelligence Community**
Refers to the following organizations:
- DL1.1.14.4. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- DL1.1.14.5. The Bureau of Intelligence and Research of the Department of State.
- DL1.1.14.6. The intelligence elements of the Army, the Navy, the Air Force and the Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.

**DL1.1.15. International Narcotics Activities**
Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with Sections 811 and 812 of title 21, United States Code.
DL1.1.16. International Terrorist Activities
Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

DL1.1.17. Lawful Investigation
An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction; if it is conducted by a DoD Component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security); and if the investigation is conducted in accordance with applicable law and policy, including E.O. 12333 and this Regulation.

DL1.1.18. Personnel Security
Measures designed to insure that persons employed, or being considered for employment, in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

DL1.1.19. Personnel Security Investigation:
- DL1.1.19.1. An inquiry into the activities of a person granted access to intelligence or other classified information; or a person who is being considered for access to intelligence or other classified information, including persons who are granted or may be granted access to facilities of DoD intelligence components; or a person to be assigned or retained in a position with sensitive duties. The investigation is designed to develop information pertaining to the suitability, eligibility, and trustworthiness of the individual with respect to loyalty, character, emotional stability and reliability.
- DL1.1.19.2. Inquiries and other activities directed against DoD employees or members of a Military Service to determine the facts of possible voluntary or involuntary compromise of classified information by them.
- DL1.1.19.3. The collection of information about or from military personnel in the course of tactical training exercises for security training purposes.
DL1.1.20. Physical Security
The physical measures taken to prevent unauthorized access to, and prevent the
damage or loss of, equipment, facilities, materiel and documents; and measures
undertaken to protect DoD personnel from physical threats to their safety.

DL1.1.21. Physical Security Investigation
All inquiries, inspections, or surveys of the effectiveness of controls and
procedures designed to provide physical security; and all inquiries and other
actions undertaken to obtain information pertaining to physical threats to DoD
personnel or property.

DL1.1.22. Reasonable Belief
A reasonable belief arises when the facts and circumstances are such that a
reasonable person would hold the belief. Reasonable belief must rest on facts and
circumstances that can be articulated; "hunches" or intuitions are not sufficient.
Reasonable belief can be based on experience, training, and knowledge in foreign
intelligence or counterintelligence work applied to facts and circumstances at
hand, so that a trained and experienced "reasonable person" might hold a
reasonable belief sufficient to satisfy this criterion when someone unfamiliar with
foreign intelligence or counterintelligence work might not.

DL1.1.23. Signals Intelligence
A category of intelligence including communications intelligence, electronic
intelligence, and foreign instrumentation signals intelligence, either individually
or in combination.

DL1.1.24. United States
When used to describe a place, the term shall include the territories under the
sovereignty of the United States.

DL1.1.25. United States Person
DL1.1.25.1. The term "United States person" means:
- DL1.1.25.1.1. A United States citizen;
- DL1.1.25.1.2. An alien known by the DoD intelligence component
  concerned to be a permanent resident alien;
- DL1.1.25.1.3. An unincorporated association substantially composed of
  United States citizens or permanent resident aliens;
- DL1.1.25.1.4. A corporation incorporated in the United States, except for a
corporation directed and controlled by a foreign government or
governments. A corporation or corporate subsidiary incorporated abroad,
even if partially or wholly owned by a corporation incorporated in the
United States, is not a United States person.

DL1.1.25.2. A person or organization outside the United States shall be presumed
not to be a United States person unless specific information to the contrary is
obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained.

DL1.1.25.3. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.
C1. CHAPTER 1: PROCEDURE 1. GENERAL PROVISIONS

C1.1. APPLICABILITY AND SCOPE
C1.1.1. These procedures apply only to "DoD intelligence components," as defined in the Definitions Section. Procedures 2 through 4 provide the sole authority by which such components may collect, retain and disseminate information concerning United States persons. Procedures 5 through 10 set forth applicable guidance with respect to the use of certain collection techniques to obtain information for foreign intelligence and counterintelligence purposes. Authority to employ such techniques shall be limited to that necessary to perform functions assigned the DoD intelligence component concerned. Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities.

C1.1.2. The functions of DoD intelligence components not specifically addressed herein shall be carried out in accordance with applicable policy and procedure.

C1.1.3. These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcement procedures.

C1.1.4. DoD intelligence components shall not request any person or entity to undertake any activity forbidden by Executive Order 12333 (reference (a)).

C1.2. PURPOSE
The purpose of these procedures is to enable DoD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

C1.3. INTERPRETATION
C1.3.1. These procedures shall be interpreted in accordance with their stated purpose.

C1.3.2. All defined terms appear in the Definitions Section. Additional terms, not otherwise defined, are explained in the text of each procedure, as appropriate.
C1.3.3. All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned. Questions that cannot be resolved in this manner shall be referred to the General Counsel of the Military Department concerned, or, as appropriate, the General Counsel of the Department of Defense for resolution.

C1.4. EXCEPTIONS TO POLICY
Requests for exception to the policies and procedures established herein shall be made in writing to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense and, if required, the Attorney General for any such exception.

C1.5. AMENDMENT
Requests for amendment of these procedures shall be made to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense, and, if required, the Attorney General, for any such amendment.
C2. CHAPTER 2: PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

C2.1. APPLICABILITY AND SCOPE
This procedure specifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information. Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques.

C2.2. EXPLANATION OF UNDEFINED TERMS

C2.2.1. When Information is Considered to be “Collected”
Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

C2.2.2. “Cooperating Sources”
Cooperating sources means persons or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information, at the request of such components or on their own initiative. These include Government Agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments.

C2.2.3. “Domestic Activities”
Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization, or person.

C2.2.4. “Overt”
Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that he is providing such information to the Department of Defense or a component thereof.

C2.3. TYPES OF INFORMATION THAT MAY BE COLLECTED ABOUT UNITED STATES PERSONS
Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:

C2.3.1. Information Obtained With Consent
Information may be collected about a United States person who consents to such collection.

C2.3.2. Publicly Available Information
Information may be collected about a United States person if it is publicly available.

C2.3.3. Foreign Intelligence
Subject to the special limitation contained in section C2.5., below, information may be collected about a United States person if the information constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are:

- C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;
- C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;
- C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;
- C2.3.3.4. Persons who are reasonably believed to be prisoners of war; missing in action; or are the targets, the hostages, or victims of international terrorist organizations; or
- C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

C2.3.4. Counterintelligence
Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:

- C2.3.4.1. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.
- C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

C2.3.5. Potential Sources of Assistance to Intelligence Activities
Information may be collected about United States persons reasonably believed to be potential sources of intelligence, or potential sources of assistance to intelligence activities, for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

C2.3.6. Protection of Intelligence Sources and Methods
Information may be collected about a United States person who has access to, had access to, or is otherwise in possession of, information that reveals foreign intelligence and counterintelligence sources or methods, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information; provided that within the United States, intentional collection of such information shall be limited to persons who are:

- C2.3.6.1. Present and former DoD employees;
- C2.3.6.2. Present or former employees of a present or former DoD contractor; and
- C2.3.6.3. Applicants for employment at the Department of Defense or at a contractor of the Department of Defense.

C2.3.7. Physical Security
Information may be collected about a United States person who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors. Information may also be collected in the course of a lawful physical security investigation.

C2.3.8. Personnel Security
Information may be collected about a United States person that arises out of a lawful personnel security investigation.

C2.3.9. Communications Security
Information may be collected about a United States person that arises out of a lawful communications security investigation.

C2.3.10. Narcotics
Information may be collected about a United States person who is reasonably believed to be engaged in international narcotics activities.

C2.3.11. Threats to Safety
Information may be collected about a United States person when the information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations.

C2.3.12. Overhead Reconnaissance
Information may be collected from overhead reconnaissance not directed at specific United States persons.

C2.3.13. Administrative Purposes
Information may be collected about a United States person that is necessary for administrative purposes.
C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS

C2.4.1. Means of Collection
DoD intelligence components are authorized to collect information about United States persons by any lawful means, provided that all such collection activities shall be carried out in accordance with E.O. 12333 (reference (a)), and this Regulation, as appropriate.

C2.4.2. Least Intrusive Means
The collection of information about United States persons shall be accomplished by the least intrusive means. In general, this means the following:

- C2.4.2.1. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned;
- C2.4.2.2. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources;
- C2.4.2.3. If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General; then
- C2.4.2.4. If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought.

C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES
Within the United States, foreign intelligence concerning United States persons may be collected only by overt means unless all the following conditions are met:

- C2.5.1. The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any United States person;
- C2.5.2. Such foreign intelligence cannot be reasonably obtained by overt means;
- C2.5.3. The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI); and
- C2.5.4. The use of other than overt means has been approved in writing by the head of the DoD intelligence component concerned, or his single designee, as being consistent with these procedures. A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy).
C3. CHAPTER 3: PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

C3.1. APPLICABILITY
This procedure governs the kinds of information about United States persons that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns. It does not apply when the information in question is retained solely for administrative purposes or is required by law to be maintained.

C3.2. EXPLANATION OF UNDEFINED TERMS
The term "retention," as used in this procedure, refers only to the maintenance of information about United States persons that can be retrieved by reference to the person's name or other identifying data.

C3.3. CRITERIA FOR RETENTION
C3.3.1. Retention of Information Collected Under Procedure 2
Information about United States persons may be retained if it was collected pursuant to Procedure 2.

C3.3.2. Retention of Information Acquired Incidentally
Information about United States persons collected incidentally to authorized collection may be retained if:

- C3.3.2.1. Such information could have been collected intentionally under Procedure 2;
- C3.3.2.2. Such information is necessary to understand or assess foreign intelligence or counterintelligence;
- C3.3.2.3. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation; or
- C3.3.2.4. Such information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

C3.3.3. Retention of Information Relating to Functions of Other DoD Components or non-DoD Agencies
Information about United States persons that pertains solely to the functions of other DoD Components or Agencies outside the Department of Defense shall be retained only as necessary to transmit or deliver such information to the appropriate recipients.

C3.3.4. Temporary Retention
Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures.

C3.3.5. Retention of Other Information
Information about United States persons other than that covered by paragraphs C3.3.1. through C3.3.4., above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

C3.4. ACCESS AND RETENTION
C3.4.1. Controls On Access to Retained Information
Access within a DoD intelligence component to information about United States persons retained pursuant to this procedure shall be limited to those with a need to know.

C3.4.2. Duration of Retention
Disposition of information about United States Persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained.

C3.4.3. Information Acquired Prior to Effective Date
Information acquired prior to the effective date of this procedure may be retained by DoD intelligence components without being screened for compliance with this procedure or Executive Order 12333 (reference (a)), so long as retention was in compliance with applicable law and previous Executive orders.
C4. CHAPTER 4: PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

C4.1. APPLICABILITY AND SCOPE
This procedure governs the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information. It does not apply to information collected solely for administrative purposes; or disseminated pursuant to law; or pursuant to a court order that otherwise imposes controls upon such dissemination.

C4.2. CRITERIA FOR DISSEMINATION
Except as provided in section C4.3., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

- C4.2.1. The information was collected or retained or both under Procedures 2 and 3;
- C4.2.2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:
  - C4.2.2.1. An employee of the Department of Defense, or an employee of a contractor of the Department of Defense, and has a need for such information in the course of his or her official duties;
  - C4.2.2.2. A law enforcement entity of Federal, State, or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce;
  - C4.2.2.3. An Agency within the intelligence community; provided that within the intelligence community, information other than information derived from signals intelligence, may be disseminated to each appropriate Agency for the purpose of allowing the recipient Agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component;
  - C4.2.2.4. An Agency of the Federal Government authorized to receive such information in the performance of a lawful governmental function; or
  - C4.2.2.5. A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

C4.3. OTHER DISSEMINATION
Any dissemination that does not conform to the conditions set forth in section C4.2., above, must be approved by the legal office responsible for advising the
DoD Component concerned after consultation with the Department of Justice and General Counsel of the Department of Defense. Such approval shall be based on determination that the proposed dissemination complies with applicable laws, Executive orders, and regulations.
C5. CHAPTER 5: PROCEDURE 5. ELECTRONIC SURVEILLANCE

C5.1. PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.1.1. Applicability
This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1979 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

C5.1.2. General Rules

C5.1.2.1. Electronic Surveillance Pursuant to the Foreign Intelligence Surveillance Act

A DoD intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes only pursuant to an order issued by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978 (reference (b)), or pursuant to a certification of the Attorney General issued under the authority of Section 102(a) of the Act.

C5.1.2.2. Authority to Request Electronic Surveillance

Authority to approve the submission of applications or requests for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (reference (b)) shall be limited to the Secretary of Defense, the Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency. Applications for court orders will be made through the Attorney General after prior clearance by the General Counsel, DoD. Requests for Attorney General certification shall be made only after prior clearance by the General Counsel, DoD.

C5.1.2.3. Electronic Surveillance In Emergency Situations

C5.1.2.3.1. A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General in accordance with Section 105(e) of reference (b).
C5.1.2.3.2. The head of a DoD intelligence component may request that the DoD General Counsel seek such authority directly from the Attorney General in an emergency, if it is not feasible to submit such request through an official designated in subparagraph C5.1.2.2., above, provided the appropriate official concerned shall be advised of such requests as soon as possible thereafter.
C5.2. PART 2: ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.2.1. Applicability
This part of Procedure 5 applies to electronic surveillance, as defined in the Definitions Section, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 and the regulation of "signals intelligence activities" under Part 3 so that the intentional interception for foreign intelligence and counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts. In addition, this part governs the use of electronic, mechanical, or other surveillance devices for foreign intelligence and counterintelligence purposes against a United States person abroad in circumstances where such person has a reasonable expectation of privacy. This part does not apply to the electronic surveillance of communications of other than United States persons abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

C5.2.2. Explanation of Undefined Terms

C5.2.2.1. "Directed against a United States Person"
Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person. Electronic surveillance directed against persons who are not United States persons that results in the incidental acquisition of the communications of a United States person does not thereby become electronic surveillance directed against a United States person.

C5.2.2.2. "Outside the United States"
Electronic surveillance is "outside the United States" if the person against whom the electronic surveillance is directed is physically outside the United States, regardless of the location at which surveillance is conducted. For example, the interception of communications that originate and terminate outside the United States can be conducted from within the United States and still fall under this part rather than Part 1.

C5.2.3. Procedures
Except as provided in paragraph C5.2.5., below, DoD intelligence components may conduct electronic surveillance against a United States person who is outside the United States for foreign intelligence and counterintelligence purposes only if the surveillance is approved by the Attorney General. Requests for approval will
be forwarded to the Attorney General by an official designated in subparagraph C5.2.5.1., below. Each request shall include:

- **C5.2.3.1.** An identification or description of the target.
- **C5.2.3.2.** A statement of the facts supporting a finding that:
  - **C5.2.3.2.1.** There is probable cause to believe the target of the electronic surveillance is one of the following:
    - **C5.2.3.2.1.1.** A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;
    - **C5.2.3.2.1.2.** A person who is an officer or employee of a foreign power;
    - **C5.2.3.2.1.3.** A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this paragraph, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;
    - **C5.2.3.2.1.4.** A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
    - **C5.2.3.2.1.5.** A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.
  - **C5.2.3.2.2.** The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence.
  - **C5.2.3.2.3.** The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be obtained by other less intrusive collection techniques.
- **C5.2.3.3.** A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance.
- **C5.2.3.4.** A description of the means by which the electronic surveillance will be effected.
- **C5.2.3.5.** If physical trespass is required to effect the surveillance, a statement of facts supporting a finding that the means involve the least amount of intrusion that will accomplish the objective.
- **C5.2.3.6.** A statement of period of time, not to exceed 90 days, for which the electronic surveillance is required.
• C5.2.3.7. A description of the expected dissemination of the product of the surveillance, including a description of the procedures that will govern the retention and dissemination of communications of or concerning United States persons other than those targeted, acquired incidental to such surveillance.

C5.2.4. Electronic Surveillance in Emergency Situations
Notwithstanding paragraph C5.2.3., above, a DoD intelligence component may conduct surveillance directed at a United States person who is outside the United States in emergency situations under the following limitations:

• C5.2.4.1. Officials designated in paragraph C5.2.5., below, may authorize electronic surveillance directed at a United States person outside the United States in emergency situations, when securing the prior approval of the Attorney General is not practical because:
  o C5.2.4.1.1. The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security;
  o C5.2.4.1.2. A person's life or physical safety is reasonably believed to be in immediate danger; or C5.2.4.1.3. The physical security of a defense installation or Government property is reasonably believed to be in immediate danger.

• C5.2.4.2. Except for actions taken under subparagraph C5.2.4.1.2., above, any official authorizing such emergency surveillance shall find that one of the criteria contained in subparagraph C5.2.3.2.1., above, is met. Such officials shall notify the DoD General Counsel promptly of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results.

• C5.2.4.3. The Attorney General shall be notified by the General Counsel, DoD, as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and such other information as may be required to authorize continuation of such surveillance.

• C5.2.4.4. Electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

C5.2.5. Officials Authorized to Request and Approve Electronic Surveillance Outside the United States

• C5.2.5.1. The following officials may request approval of electronic surveillance outside the United States under paragraph C5.2.3., above, and approve emergency surveillance under paragraph C5.2.4., above:
  o C5.2.5.1.1. The Secretary and Deputy Secretary of Defense.
  o C5.2.5.1.2. The Secretaries and Under Secretaries of the Military Departments.
C5.2.5.1.3. The Director and Deputy Director of the National Security Agency/Chief, Central Security Service.

C5.2.5.2. Authorization for emergency electronic surveillance under paragraph C5.2.4., may also be granted by:

- C5.2.5.2.1. Any general or flag officer at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered, or
- C5.2.5.2.2. The Deputy Director for Operations, National Security Agency.

C5.3. PART 3: SIGNALS INTELLIGENCE ACTIVITIES

C5.3.1. Applicability and Scope

- C5.3.1.1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection, retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.

- C5.3.1.2. This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the Attorney General. That regulation shall provide that signals intelligence activities that constitute electronic surveillance, as defined in Parts 1, and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the Attorney General.

C5.3.2. Explanation of Undefined Terms

C5.3.2.1. “Communications concerning a United States person”

- Communications concerning a United States person are those in which the United States person is identified in the communication. A United States person is identified when the person's name, unique title, address or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Monroe Doctrine," is not an identification of a United States person.

C5.3.2.2. “Interception”
Interception means the acquisition by the United States Signals Intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signals.

C5.3.2.3. “Military tactical communication”

Military tactical communications means United States and allied military exercise communications within the United States and abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

C5.3.2.4. SIGINT Guidelines for Determining whether a person is a “United States Person.”

For purposes of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person:
- C5.3.2.4.1. Person Known to be Currently in the United States
  - A person known to be currently in the United States will be treated as a United States person unless the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.
- C5.3.2.4.2. Person Known to be Currently Outside the United States
  - A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.
- C5.3.2.4.3. Circumstances in which a Person Known to be an Alien Admitted for Permanent Residence may be assumed to have lost status as a United States Person
  - A person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is
not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien’s entry into the United States. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

- C5.3.2.4.4. Unincorporated Association whose Headquarters are located outside the United States
  - An unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence.

C5.3.2.5. “United States Signals Intelligence System”

- United States Signals Intelligence System means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the Military Services authorized to conduct signals intelligence and such other entities (other than the Federal Bureau of Investigation) as are authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence. FBI activities are governed by procedures promulgated by the Attorney General.

C5.3.3. Procedures

C5.3.3.1. Foreign Communications

- The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure.

C5.3.3.2. Military Tactical Communications

- The United States Signals Intelligence System may collect, process, retain, and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure.
C5.3.3.2.1. Collection

- Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercises.

C5.3.3.2.2. Retention and Processing

- Military tactical communications may be retained and processed without deletion of references to United States persons who are participants in, or are otherwise mentioned in exercise-related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible.

C5.3.3.2.3. Dissemination

- Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating in or conducting reviews and critiques of such exercise.

C5.4. PART 4: TECHNICAL SURVEILLANCE COUNTERMEASURES

C5.4.1. Applicability and Scope
This part of Procedure 5 applies to the use of electronic equipment to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements Section 105(f)(2) of the Foreign Intelligence Surveillance Act (reference (b)).

C5.4.2. Explanation of Undefined Terms
The term technical surveillance countermeasures refers to activities authorized pursuant to DoD Directive 5200.29 (reference (c)), and, as used in this procedure, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, or for determining the susceptibility of electronic equipment to unlawful electronic surveillance.

C5.4.3. Procedures
A DoD intelligence component may use technical surveillance countermeasures that involve the incidental acquisition of the nonpublic communications of United States persons without their consent, provided:

Page 1272
C5.4.3.1. The use of such countermeasures has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken;

C5.4.3.2. The use of such countermeasures is limited in that necessary to determine the existence and capability of such equipment; and

C5.4.3.3. Access to the content of communications acquired during the use of countermeasures is limited to persons involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use. However, if the content is acquired within the United States, only information that is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (d)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated only for these purposes. If acquired outside the United States, information that indicates a violation of Federal law, including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities. A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained.

C5.5. PART 5: DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENT

C5.5.1. Applicability
This part of Procedure 5 applies to developing, testing, or calibrating electronic equipment that can intercept or process communications and noncommunications signals. It also includes research and development that needs electronic communications as a signal source.

C5.5.2. Procedures

C5.5.2.1. Signals Authorized for Use

C5.5.2.1.1. The following may be used without restriction:

- C5.5.2.1.1.1. Laboratory-generated signals.
- C5.5.2.1.1.2. Communications signals with the consent of the communicator.
- C5.5.2.1.1.3. Communications in the commercial or public service broadcast bands.
- C5.5.2.1.1.4. Communications transmitted between terminals located outside of the United States not used by any known United States person.
- C5.5.2.1.1.5. Noncommunications signals (including telemetry, and radar).

C5.5.2.1.2. Communications subject to lawful electronic surveillance under the provisions of Parts 1, 2, or 3, of this procedure may be
used subject to the minimization procedures applicable to such surveillance.

- C5.5.2.1.3. Any of the following may be used subject to the restrictions of subparagraph C5.5.2.2., below.
  - C5.5.2.1.3.1. Communications over official Government communications circuits with consent from an appropriate official of the controlling agency.
  - C5.5.2.1.3.2. Communications in the citizens and amateur-radio bands.

- C5.5.2.1.4. Other signals may be used only when it is determined that it is not practical to use the signals described above and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. The restrictions of subparagraph C5.5.2.2., below, will apply in such cases. The Attorney General must approve use of signals pursuant to this subsection for the purpose of development, testing, or calibration when the period of use exceeds 90 days. When Attorney General approval is required, the DoD intelligence component shall submit a test proposal to the General Counsel, DoD, or the NSA General Counsel for transmission to the Attorney General for approval. The test proposal shall state the requirement for a period beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity.

C5.5.2.2. Restrictions

- For signals described in subparagraphs C5.5.2.1.3. and C5.5.2.1.4., above, the following restrictions apply:
  - C5.5.2.2.1. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in paragraph C5.5.1., above.
  - C5.5.2.2.2. No particular United States person shall be targeted intentionally without consent.
  - C5.5.2.2.3. The content of any communication shall:
    - C5.5.2.2.3.1. Be retained only when actually needed for the purposes referred to in paragraph C5.5.1., above;
    - C5.5.2.2.3.2. Be disseminated only to persons conducting the activity; and
    - C5.5.2.2.3.3. Be destroyed immediately upon completion of the activity.
  - C5.5.2.2.4. The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes outlined in paragraph C5.5.1., above, or for collection
avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment provided such dissemination and use are limited to the purposes outlined in paragraph C5.5.1., or collection avoidance purposes. No content of any communication may be retained or used other than as provided in subparagraph C5.5.2.2.3., above.

C5.6. PART 6: TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

C5.6.1. Applicability
This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment. It does not apply to the interception of communications with the consent of one of the parties to the communication or to the training of intelligence personnel by non-intelligence components.

C5.6.2. Procedures

C5.6.2.1. Training Guidance

- The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment shall include guidance concerning the requirements and restrictions of the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and E.O. 12333 (reference (a)), with respect to the unauthorized acquisition and use of the content of communications of United States persons.

C5.6.2.2. Training Limitations

- C5.6.2.2.1. Except as permitted by paragraph C5.6.2.2.2. and C5.6.2.2.3., below, the use of electronic communications and surveillance equipment for training purposes is permitted, subject to the following limitations:
  - C5.6.2.2.1.1. To the maximum extent practical, use of such equipment for training purposes shall be directed against communications that are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure.
  - C5.6.2.2.1.2. The contents of private communications of nonconsenting United States persons may not be acquired
aurally unless the person is an authorized target of electronic surveillance.

- C5.6.2.2.1.3. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

- C5.6.2.2.2. Public broadcasts, distress signals, or official U.S. Government communications may be monitored, provided that when Government Agency communications are monitored, the consent of an appropriate official is obtained.

- C5.6.2.2.3. Minimal acquisition of information is permitted as required for calibration purposes.

C5.6.2.3. Retention and Dissemination

- Information collected during training that involves communications described in subparagraph C5.6.2.2.1.1., above, shall be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance. Information collected during training that does not involve communications described in subparagraph C5.6.2.2.1.1., above, or that is acquired inadvertently, shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This limitation does not apply to distress signals.

C5.7. PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS

C5.7.1. Applicability and Scope
This part of Procedure 5 applies to the conduct of vulnerability surveys and hearability surveys by DoD intelligence components.

C5.7.2. Explanation of Undefined Terms

C5.7.2.1. “Vulnerability Survey”

- The term vulnerability survey refers to the acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.

C5.7.2.2. “Hearability Survey”

- The term hearability survey refers to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if
reception is possible, to determine the hearability of reception over time.

C5.7.3. Procedures

C5.7.3.1. Conduct of Vulnerability Surveys

- Nonconsensual surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of transmission facilities of communications common carriers, other private commercial entities, and entities of the federal government, subject to the following limitations:
  - C5.7.3.1.1. No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee.
  - C5.7.3.1.2. No transmission may be acquired aurally.
  - C5.7.3.1.3. No content of any transmission may be acquired by any means.
  - C5.7.3.1.4. No transmissions may be recorded.
  - C5.7.3.1.5. No report or log may identify any United States person or entity except to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

C5.7.3.2. Conduct of Hearability Surveys

- The Director, National Security Agency, may conduct, or may authorize the conduct by other Agencies, of hearability surveys of telecommunications that are transmitted in the United States.
  - C5.7.3.2.1. Collection. When practicable, consent will be secured from the owner or user of the facility against which the hearability survey is to be conducted prior to the commencement of the survey.
  - C5.7.3.2.2. Processing and Storage. Information collected during a hearability survey must processed and stored as follows:
    - C5.7.3.2.2.1. The content of communications may not be recorded or included in any report.
    - C5.7.3.2.2.2. No microwave transmission may be demultiplexed or demodulated for any purpose.
C5.7.3.2.2.3. No report or log may identify any person or entity except to the extent of identifying the transmission facility that can be intercepted from the intercept site. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the hearability survey has been conducted, the identity of such users may be obtained provided such identities may not be obtained from the contents of the transmissions themselves.

C5.7.3.2.3. Dissemination. Reports may be disseminated only within the U.S. Government. Logs may not be disseminated unless required to verify results contained in reports.
C6. CHAPTER 6: PROCEDURE 6. CONCEALED MONITORING

C6.1. APPLICABILITY AND SCOPE

C6.1.1. Where no warrant would be required
This procedure applies to concealed monitoring only for foreign intelligence and counterintelligence purposes conducted by a DoD intelligence component within the United States or directed against a United States person who is outside the United States where the subject of such monitoring does not have a reasonable expectation of privacy, as explained in section 6.2., below, and no warrant would be required if undertaken for law enforcement purposes.

C6.1.2. Situations where a warrant would be required shall be treated as “Electronic surveillance”
Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure.

C6.1.3. Concealed monitoring of U.S. Person Abroad
Concealed monitoring for foreign intelligence and counterintelligence purposes of a United States person abroad where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance outside the United States" under Part 2 of Procedure 5, and processed pursuant to that procedure.

C6.1.4. Concealed monitoring involving signals intelligence
Concealed monitoring for foreign intelligence and counterintelligence purposes when the monitoring is a signals intelligence activity shall be conducted pursuant to Part 3 of Procedure 5.

C6.2. EXPLANATION OF UNDEFINED TERMS

C6.2.1. “Concealed Monitoring”
Concealed monitoring means targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time.

C6.2.2. Monitoring “within the United States”
Monitoring is within the United States if the monitoring device, or the target of the monitoring, is located within the United States.

C6.2.3. Concealed Monitoring where the subject has a reasonable expectation of privacy
Whether concealed monitoring is to occur where the subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office responsible for advising the DoD intelligence component concerned. Reasonable expectation of privacy is the extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to monitoring by electronic, optical, or mechanical devices. For example, there are ordinarily reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal working conditions. Conversely, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed; however, such a person ordinarily would have an expectation of privacy within his or her residence.

C6.3. PROCEDURES
C6.3.1. Limitations On Use of Concealed Monitoring
Use of concealed monitoring under circumstances when the subject of such monitoring has no reasonable expectation of privacy is subject to the following limitations:

C6.3.1.1. Inside the United States

- Within the United States, a DoD intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by the Department of Defense or otherwise in the course of an investigation conducted pursuant to the Agreement Between the Secretary of Defense and the Attorney General (reference (g)).

C6.3.1.2. Outside the United States

- Outside the United States, such monitoring may be conducted on installations and facilities owned or leased by the Department of Defense. Monitoring outside such facilities shall be conducted after coordination with appropriate host country officials, if such coordination is required by the governing Status of Forces Agreement, and with the Central Intelligence Agency.

C6.3.2. Required Determination
Concealed monitoring conducted under paragraph C6.3.1., requires approval by an official designated in paragraph C6.3.3., below, based on a determination that
such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions, and does not constitute electronic surveillance under Parts 1 or 2 of Procedure 5.

C6.3.3. Officials Authorized to Approve Concealed Monitoring
Officials authorized to approve concealed monitoring under this procedure include the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Director, National Security Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Director, Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, U.S. Air Force; the Commanding General, Army Intelligence and Security Command; the Director, Naval Investigative Service; and the Commanding Officer, Air Force Office of Special Investigations.
C7. CHAPTER 7: PROCEDURE 7. PHYSICAL SEARCHES

C7.1. APPLICABILITY
This procedure applies to nonconsensual physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes. DoD intelligence components may provide assistance to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12.

C7.2. EXPLANATION OF UNDEFINED TERMS
Physical search means any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. The term also does not include any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to Parts 1 and 2 of Procedure 5.

C7.3. PROCEDURES
C7.3.1. Nonconsensual Physical Searches Within the United States

C7.3.1.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes

- The counterintelligence elements of the Military Departments are authorized to conduct nonconsensual physical searches in the United States for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.1.2., below.

C7.3.1.2. Other Nonconsensual Physical Searches

- Except as permitted by section C7.1., above, DoD intelligence components may not conduct nonconsensual physical searches of persons and property within the United States for foreign intelligence or counterintelligence purposes. DoD intelligence components may, however, request the FBI to conduct such...
searches. All such requests, shall be in writing; shall contain the information required in subparagraphs C7.3.2.2.1., through C7.3.2.2.6., below; and be approved by an official designated in subparagraph C7.3.2.2.3., below. A copy of each such request shall be furnished the General Counsel, DoD.

C7.3.2. Nonconsensual Physical Searches Outside the United States

C7.3.2.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes.

- The counterintelligence elements of the Military Departments may conduct nonconsensual physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.2.2.2., below.

C7.3.2.2. Other Nonconsensual Physical Searches

- DoD intelligence components may conduct other nonconsensual physical searches for foreign intelligence and counterintelligence purposes of the person or property of United States persons outside the United States only pursuant to the approval of the Attorney General. Requests for such approval will be forwarded by a senior official designated in subparagraph C7.3.2.3., below, to the Attorney General and shall include:
  - C7.3.2.2.1. An identification of the person or description of the property to be searched.
  - C7.3.2.2.2. A statement of facts supporting a finding that there is probable cause to believe the subject of the search is:
    - C7.3.2.2.2.1. A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities;
    - C7.3.2.2.2.2. A person who is an officer or employee of a foreign power;
C7.3.2.2.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power does not justify a nonconsensual physical search without evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C7.3.2.2.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C7.3.2.2.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

• C7.3.2.2.3. A statement of facts supporting a finding that the search is necessary to obtain significant foreign intelligence or counterintelligence.
• C7.3.2.2.4. A statement of facts supporting a finding that the significant foreign intelligence or counterintelligence expected to be obtained could not be obtained by less intrusive means.
• C7.3.2.2.5. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search.
• C7.3.2.2.6. A description of the extent of the search and a statement of facts supporting a finding that the search will involve the least amount of physical intrusion that will accomplish the objective sought.
• C7.3.2.2.7. A description of the expected dissemination of the product of the search, including a description of the procedures that will govern the retention and dissemination of information about United States persons acquired incidental to the search.

C7.3.2.3. Officials that may request approval of nonconsensual physical searches under subparagraph C7.3.2.2.

• Requests for approval of nonconsensual physical searches under subparagraph C7.3.2.2., must be made by:
  o C7.3.2.3.1. The Secretary or the Deputy Secretary of Defense;
  o C7.3.2.3.2. The Secretary or the Under Secretary of a Military Department;
  o C7.3.2.3.3. The Director, National Security Agency; or
  o C7.3.2.3.4. The Director, Defense Intelligence Agency.
C8. CHAPTER 8: PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

C8.1. APPLICABILITY
This procedure applies to the opening of mail in United States postal channels, and the use of mail covers with respect to such mail, for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from United States persons where such activity is conducted outside the United States and such mail is not in United States postal channels.

C8.2. EXPLANATION OF UNDEFINED TERMS
C8.2.1. “Mail within United States Postal Channels”
Mail Within United States Postal Channels includes:

- C8.2.1.1. Mail while in transit within, among, and between the United States, its territories and possessions (including mail of foreign origin that is passed by a foreign postal administration, to the United States Postal Service for forwarding to a foreign postal administration under a postal treaty or convention, and mail temporarily in the hands of the United States Customs Service or the Department of Agriculture), Army-Air Force (APO) and Navy (FPO) post offices, and mail for delivery to the United Nations, NY; and
- C8.2.1.2. International mail en route to an addressee in the United States or its possessions after passage to United States Postal Service from a foreign postal administration or en route to an addressee abroad before passage to a foreign postal administration. As a rule, mail shall be considered in such postal channels until the moment it is delivered manually in the United States to the specific addressee named on the envelope, or his authorized agent.

C8.2.2. “To examine mail”
To examine mail means to employ a mail cover with respect to such mail.

C8.2.3. “Mail cover”
Mail cover means the process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service.

C8.3. PROCEDURES
C8.3.1. Searches of Mail Within United States Postal Channels
- C8.3.1.1. Applicable postal regulations do not permit DoD intelligence components to detain or open first-class mail within United States postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service.
• C8.3.1.2. DoD intelligence components may request appropriate U.S. postal authorities to inspect, or authorize the inspection, of the contents of second-, third-, or fourth-class mail in United States postal channels, for such purposes, in accordance with applicable postal regulations. Such components may also request appropriate U.S. postal authorities to detain, or permit the detention of, mail that may become subject to search under this section, in accordance with applicable postal regulations.

C8.3.2. Searches of Mail Outside United States Postal Channels
• C8.3.2.1. DoD intelligence components are authorized to open mail to or from a United States person that is found outside United States postal channels only pursuant to the approval of the Attorney General. Requests for such approval shall be treated as a request for a nonconsensual physical search under subparagraph C7.3.2.2., of Procedure 7.
• C8.3.2.2. Heads of DoD intelligence components may authorize the opening of mail outside U.S. postal channels when both the sender and intended recipient are other than United States persons if such searches are otherwise lawful and consistent with any Status of Forces Agreement that may be in effect.

C8.3.3. Mail Covers
• C8.3.3.1. DoD intelligence components may request U.S. postal authorities to examine mail in U.S. postal channels, for counterintelligence purposes, in accordance with applicable postal regulations.
• C8.3.3.2. DoD intelligence components may also request mail covers with respect to mail to or from a United States person that is outside U.S. postal channels, in accordance with appropriate law and procedure of the host government, and any Status of Forces Agreement that may be effect.
C9. CHAPTER 9: PROCEDURE 9. PHYSICAL SURVEILLANCE

C9.1. APPLICABILITY
This procedure applies only to the physical surveillance of United States persons by DoD intelligence components for foreign intelligence and counterintelligence purposes. This procedure does not apply to physical surveillance conducted as part of a training exercise when the subjects are participants in the exercise.

C9.2. EXPLANATION OF UNDEFINED TERMS
The term physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance.

C9.3. PROCEDURES
C9.3.1. Criteria for Physical Surveillance In the United States
Within the United States, DoD Intelligence components may conduct nonconsensual physical surveillances for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence component concerned; present or former contractors of such components or their present or former employees; applicants for such employment or contracting; or military persons employed by a non-intelligence element of a Military Service. Any physical surveillance within the United States that occurs outside a DoD installation shall be coordinated with the FBI and other law enforcement agencies, as may be appropriate.

C9.3.2. Criteria for Physical Surveillance Outside the United States
Outside the United States, DoD Intelligence components may conduct nonconsensual physical surveillance of United States persons in one of the categories identified in paragraph C9.3.1., above. In addition, such components may conduct physical surveillance of other United States persons in the course of a lawful foreign intelligence or counterintelligence investigation, provided:

- C9.3.2.1. Such surveillance is consistent with the laws and policy of the host government and does not violate any Status of Forces Agreement that may be in effect;
- C9.3.2.2. That physical surveillance of a United States person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot be obtained by other means.

C9.3.3. Required Approvals for Physical Surveillance
- C9.3.3.1. Persons Within DoD Investigative Jurisdiction. Physical surveillances within the United States or that involve United States persons within DoD investigative jurisdiction overseas may be approved
by the head of the DoD intelligence component concerned or by designated senior officials of such components in accordance with this procedure.

- **C9.3.3.2. Persons Outside DoD Investigative Jurisdiction.** Outside the United States, physical surveillances of United States persons who are not within the investigative jurisdiction of the DoD intelligence component concerned will be forwarded through appropriate channels to the Deputy Under Secretary of Defense (Policy) for approval. Such requests shall indicate coordination with the Central Intelligence Agency.
C10. CHAPTER 10: PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

C10.1. APPLICABILITY
This procedure applies to participation by employees of DoD intelligence components in any organization within the United States, or any organization outside the United States that constitutes a United States person, when such participation is on behalf of any entity of the intelligence community. These procedures do not apply to participation in organizations for solely personal purposes.

C10.2. EXPLANATION OF UNDEFINED TERMS
C10.2.1. “Domestic Activities”
Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization or person.

C10.2.2. “Organization”
The term organization includes corporations and other commercial organizations, academic institutions, clubs, professional societies, associations, and any other group whose existence is formalized in some manner or otherwise functions on a continuing basis.

C10.2.3. “Organization within the United States”
An organization within the United States means all organizations physically located within the geographical boundaries of the United States whether or not they constitute a United States persons. Thus, a branch, subsidiary, or office of an organization within the United States, which is physically located outside the United States, is not considered as an organization within the United States.

C10.2.4. “Participation”
Participation refers to any action undertaken within the structure or framework of the organization involved. Such actions include serving as a representative or agent of the organization; acquiring membership; attending meetings not open to the public, including social functions for the organization as a whole; carrying out the work or functions of the organization; and contributing funds to the organization other than in payment for goods or services. Actions taken outside the organizational framework, however, do not constitute participation. Thus, attendance at meetings or social gatherings that involve organization members, but are not functions or activities of the organization itself does not constitute participation.

C10.2.5. “Participation on behalf of an agency within the intelligence community”
Participation is on behalf of an agency within the intelligence community when an employee is tasked or requested to take action within an organization for the benefit of such agency. Such employee may already be a member of the organization or may be asked to join. Actions undertaken for the benefit of an intelligence agency include collecting information, identifying potential sources or contacts, or establishing and maintaining cover. If a cooperating source furnishes information to an intelligence agency that he or she obtained by participation within an organization, but was not given prior direction or tasking by the intelligence agency to collect such information, then such participation was not on behalf of such agency.

C10.2.6. “Participation solely for personal purposes”
Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit.

C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION
Except as permitted herein, employees of DoD intelligence components may participate on behalf of such components in organizations within the United States, or in organizations outside the United States that constitute United States persons, only if their affiliation with the intelligence component concerned is disclosed to an appropriate official of the organization in accordance with section C10.4., below. Participation without such disclosure is permitted only if it is consistent with the limitations set forth in paragraph C10.3.1., below, and has been approved in accordance with paragraph C10.3.2., below.

C10.3.1. Limitations On Undisclosed Participation
• C10.3.1.1. Lawful Purpose. No undisclosed participation shall be permitted under this procedure unless it is essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of the collecting DoD intelligence component.
• C10.3.1.2. Limitations On Use of Undisclosed Participation for Foreign Intelligence Purposes Within the United States. Undisclosed participation may not be authorized within the United States for the purpose of collecting foreign intelligence from or about a United States person, nor to collect information necessary to assess United States persons as potential sources of assistance to foreign intelligence activities. This does not preclude the collection of information about such persons, volunteered by cooperating sources participating in organizations to which such persons belong, however, if otherwise permitted by Procedure 2.
• C10.3.1.3. Duration of Participation. Authorization to participate under subparagraphs C10.3.2.1., and C10.3.2.2., shall be limited to the period covered by such participation, which shall be no longer than 12 months. Participation that lasts longer than 12 months shall be reapproved by the appropriate official on an annual basis in accordance with this procedure.
• C10.3.1.4. Participation for the Purpose of Influencing the Activities of the Organization or Its Members. No participation under this procedure shall be authorized for the purpose of influencing the activities of the organization in question, or its members, unless such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power. Any DoD intelligence component that desires to undertake participation for such purpose shall forward its request to the Deputy Under Secretary of Defense (Policy) setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity. Such participation may be approved by the DUSD(P) with the concurrence of the General Counsel, DoD.

C10.3.2. Required Approvals
• C10.3.2.1. Undisclosed Participation That May Be Approved Within the DoD Intelligence Component. Undisclosed participation on behalf of a DoD intelligence component may be authorized with such component under the following circumstances:
  o C10.3.2.1.1. Participation in meetings open to the public. For purposes of this section, a seminar or conference sponsored by a professional organization that is open to persons of a particular profession, whether or not they are members of the organization itself or have received a special invitation, shall be considered a meeting open to the public.
  o C10.3.2.1.2. Participation in organizations that permit other persons acknowledged to the organization to be employees of the U.S. Government to participate.
  o C10.3.2.1.3. Participation in educational or professional organizations for the purpose of enhancing the professional skills, knowledge, or capabilities of employees.
  o C10.3.2.1.4. Participation in seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar types of meetings, sponsored by organizations in which the employee is a member, has been invited to participate, or when the sponsoring organization does not require disclosure of the participants' employment affiliations, for the purpose of collecting significant foreign intelligence that is generally made available to participants at such meetings, and does not involve the domestic activities of the organization or its members.
• C10.3.2.2. Participation That May Be Approved By Senior Intelligence Officials. Undisclosed participation may be authorized by the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Commanding General, U.S. Army Intelligence and Security Command;
the Director of Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, United States Air Force; the Director, Naval Investigative Service; the Commanding Officer, Air Force Office of Special Investigations; or their single designees, for the following purposes:

- C10.3.2.2.1. To collect significant foreign intelligence outside the United States, or from or about other than United States persons within the United States, provided no information involving the domestic activities of the organization or its members may be collected.

- C10.3.2.2.2. For counterintelligence purposes, at the written request of the Federal Bureau of Investigation.

- C10.3.2.2.3. To collect significant counterintelligence about other than United States persons, or about United States persons who are within the investigative jurisdiction of the Department of Defense, provided any such participation that occurs within the United States shall be coordinated with the Federal Bureau of Investigation.

- C10.3.2.2.4. To collect information necessary to identify and assess other than United States persons as potential sources of assistance for foreign intelligence and counterintelligence activities.

- C10.3.2.2.5. To collect information necessary to identify United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

- C10.3.2.2.6. To develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities.

- C10.3.2.2.7. Outside the United States, to assess United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

**C10.4. DISCLOSURE REQUIREMENT**

C10.4.1. Disclosure of the intelligence affiliation of an employee of a DoD intelligence component shall be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization concerned.

C10.4.2. Disclosure may be made by the DoD intelligence component involved, an authorized DoD official, or by another component of the Intelligence Community that is otherwise authorized to take such action on behalf of the DoD intelligence component concerned.
C11. CHAPTER 11: PROCEDURE 11. CONTRACTING
FOR GOODS AND SERVICES

C11.1. APPLICABILITY
This procedure applies to contracting or other arrangements with United States persons for the procurement of goods and services by DoD intelligence components within the United States. This procedure does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. The latter situation is governed by Procedure 10.

C11.2. PROCEDURES
C11.2.1. Contracts with Academic Institutions
DoD intelligence components may enter into a contract for goods or services with an academic institution only if prior to the making of the contract, the intelligence component has disclosed to appropriate officials of the academic institution the fact of sponsorship by a DoD intelligence component.

C11.2.2. Contracts with Commercial Organizations, Private Institutions, and Individuals
Contracting by or for a DoD intelligence component with commercial organizations, private institutions, or private individuals within the United States may be done without revealing the sponsorship of the intelligence component if:

- C11.2.2.1. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities; or
- C11.2.2.2. There is a written determination by the Secretary or the Under Secretary of a Military Department, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, or the Deputy Under Secretary of Defense (Policy) that the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned.

C11.3. EFFECT OF NONCOMPLIANCE
No contract shall be void or voidable for failure to comply with this procedure.
C12. CHAPTER 12: PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES

C12.1. APPLICABILITY
This procedure applies to the provision of assistance by DoD intelligence components to law enforcement authorities. It incorporates the specific limitations on such assistance contained in E.O. 12333 (reference (a)), together with the general limitations and approval requirements of DoD Directive 5525.5 (reference (i)).

C12.2. PROCEDURES
C12.2.1. Cooperation with Law Enforcement Authorities
Consistent with the limitations contained in DoD Directive 5525.5 (reference (i)), and paragraph C12.2.2., below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:
- C12.2.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;
- C12.2.1.2. Protecting DoD employees, information, property, and facilities; and
- C12.2.1.3. Preventing, detecting, or investigating other violations of law.

C12.2.2. Types of Permissible Assistance
DoD intelligence components may provide the following types of assistance to law enforcement authorities:
- C12.2.2.1. Incidentally acquired information reasonably believed to indicate a violation of Federal law shall be provided in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a));
- C12.2.2.2. Incidentally acquired information reasonably believed to indicate a violation of State, local, or foreign law may be provided in accordance with procedures adopted by the Heads of DoD Components;
- C12.2.2.3. Specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to, Enclosure 3 of DoD Directive 5525.5 (reference (i)); and
- C12.2.2.4. Personnel who are employees of DoD intelligence components may be assigned to assist Federal law enforcement authorities, and, when lives are endangered, State and local law enforcement authorities, provided such use is consistent with, and has been approved by an official authorized pursuant to, Enclosure 4 of DoD Directive 5525.5 (reference (i)). Such official shall ensure that the General Counsel of the providing DoD Component concurs in such use.
C12.2.2.5. Assistance may be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policy and applicable Status of Forces Agreements; provided, that DoD intelligence components may not request or participate in activities of such agencies undertaken against United States persons that would not be permitted such components under these procedures.
EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

C13.1. APPLICABILITY
This procedure applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a DoD intelligence component. This procedure does not apply to experimentation on animal subjects.

C13.2. EXPLANATION OF UNDEFINED TERMS
• C13.2.1. Experimentation in this context means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.
• C13.2.2. Experimentation is conducted on behalf of a DoD intelligence component if it is conducted under contract to that component or to another DoD Component for the benefit of the intelligence component or at the request of such a component regardless of the existence of a contractual relationship.
• C13.2.3. Human subjects in this context includes any person whether or not such person is a United States person.

C13.3. PROCEDURES
• C13.3.1. Experimentation on human subjects conducted by or on behalf of a DoD intelligence component may be undertaken only with the informed consent of the subject, in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects.
• C13.3.2. DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the Secretary or Deputy Secretary of Defense, or the Secretary or Under Secretary of a Military Department, as appropriate.
C14. CHAPTER 14: PROCEDURE 14. EMPLOYEE CONDUCT

C14.1. APPLICABILITY
This procedure sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this Regulation and other applicable policy. It also provides that DoD intelligence components shall ensure, as appropriate, that these policies and guidelines are made known to their employees.

C14.2. PROCEDURES
C14.2.1. Employee Responsibilities
Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by law; Executive order, including E.O. 12333 (reference (a)), and applicable DoD Directives.

C14.2.2. Familiarity With Restrictions
• C14.2.2.1. Each DoD intelligence component shall familiarize its personnel with the provisions of E.O. 12333 (reference (a)), this Regulation, and any instructions implementing this Regulation that apply to the operations and activities of such component. At a minimum, such familiarization shall contain:
  o C14.2.2.1.1. Applicable portions of Procedures 1 through 4;
  o C14.2.2.1.2. A summary of other procedures that pertains to collection techniques that are, or may be, employed by the DoD intelligence component concerned; and
  o C14.2.2.1.3. A statement of individual employee reporting responsibility under Procedure 15.

• C14.2.2.2. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IQ)) and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect that will achieve the objectives set forth in subparagraph C14.2.2.1., above.

C14.2.3. Responsibilities of the Heads of DoD Components
The Heads of DoD Components that constitute, or contain, DoD intelligence components shall:
• C14.2.3.1. Ensure that all proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to applicable Executive Branch or DoD policy are referred to the General Counsel responsible for such component.
• C14.2.3.2. Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15.
• C14.2.3.3. Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder.
• C14.2.3.4. In any case involving serious or continuing breaches of security by either DoD or non-DoD employees, recommend to the Secretary of Defense appropriate investigative actions.
• C14.2.3.5. Ensure that the General Counsel and Inspector General with responsibility for the component, as well as the General Counsel, DoD, and the ATSD(IO), have access to all information concerning the intelligence activities of that component necessary to perform their oversight responsibilities.
• C14.2.3.6. Ensure that employees cooperate fully with the Intelligence Oversight Board and its representatives.
C15. CHAPTER 15: PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE ACTIVITIES

C15.1. APPLICABILITY
This procedure provides for the identification, investigation, and reporting of questionable intelligence activities.

C15.2. EXPLANATION OF UNDEFINED TERMS
C15.2.1. “Questionable Activity”
The term "questionable activity," as used herein, refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive order or Presidential directive, including E.O. 12333 (reference (a)), or applicable DoD policy, including this Regulation.

C15.2.2. “General Counsel” and “Inspector General”
The terms "General Counsel" and "Inspector General," as used herein, refer, unless otherwise specified, to any General Counsel or Inspector General with responsibility for one or more DoD intelligence components. Unless otherwise indicated, the term "Inspector General" shall also include the ATSD(IO).

C15.3. PROCEDURES
C15.3.1. Identification
- C15.3.1.1. Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO).
- C15.3.1.2. Inspectors General, as part of their inspection of DoD intelligence components, and General Counsels, as part of their oversight responsibilities shall seek to determine if such components are involved in any questionable activities. If such activities have been or are being undertaken, the matter shall be investigated under paragraph C15.3.2., below. If such activities have been undertaken, but were not reported, the Inspector General shall also ascertain the reason for such failure and recommend appropriate corrective action.
- C15.3.1.3. Inspectors General, as part of their oversight responsibilities, shall, as appropriate, ascertain whether any organizations, staffs, or offices within their respective jurisdictions, but not otherwise specifically identified as DoD intelligence components, are being used for foreign intelligence or counterintelligence purposes to which Part 2 of E.O. 12333 (reference (a)), applies, and, if so, shall ensure the activities of such components are in compliance with this Regulation and applicable DoD policy.
- C15.3.1.4. Inspectors General, as part of their inspection of DoD intelligence components, shall ensure that procedures exist within such
components for the reporting of questionable activities, and that employees of such components are aware of their responsibilities to report such activities.

C15.3.2. Investigation

- C15.3.2.1. Each report of a questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy.

- C15.3.2.2. When appropriate, questionable activities reported to a General Counsel shall be referred to the corresponding Inspector General for investigation, and if reported to an Inspector General, shall be referred to the corresponding General Counsel to determine whether the activity is legal and consistent with applicable policy. Reports made to the DoD General Counsel or the ATSD(IO) may be referred, after consultation between these officials, to the appropriate Inspector General and General Counsel for investigation and evaluation.

- C15.3.2.3. Investigations shall be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from within the component concerned, or from other DoD Components, when necessary, to complete such investigations in a timely manner.

- C15.3.2.4. To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation.

C15.3.3. Reports

- C15.3.3.1. Each General Counsel and Inspector General shall report immediately to the General Counsel, DoD, and the ATSD(IO) questionable activities of a serious nature.

- C15.3.3.2. Each General Counsel and Inspector General shall submit to the ATSD(IO) a quarterly report describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive order or Presidential directive, or applicable DoD policy; and actions taken with respect to such activities. The reports shall also include significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system. Separate, joint, or consolidated reports may be submitted. These reports should be prepared in accordance with DoD Directive 5000.11 (reference (j)).

- C15.3.3.3. All reports made pursuant to subparagraphs C15.3.3.1., and C15.3.3.2., above, which involve a possible violation of Federal criminal law shall be considered by the General Counsel concerned in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a)).
• C15.3.3.4. The General Counsel, DoD, and the ATSD(IO) may review the findings of other General Counsels and Inspectors General with respect to questionable activities.

• C15.3.3.5. The ATSD(IO) and the General Counsel, DoD, shall report in a timely manner to the White House Intelligence Oversight Board all activities that come to their attention that are reasonably believed to be illegal or contrary to Executive order or Presidential directive. They will also advise appropriate officials of the Office of the Secretary of Defense of such activities.

• C15.3.3.6. These reporting requirements are exempt from format approval and licensing in accordance with paragraph VII.G. of Enclosure 3 to DoD Directive 5000.19 (reference (k)).
SUBJECT: DoD Intelligence Activities

References:
• DoD Directive 5143.01, “Under Secretary of Defense for Intelligence,” November 23, 2005
• Executive Order 13388, “Further Strengthening the Sharing of Terrorism Information to Protect Americans,” October 25, 2005
• through (k), see Enclosure 1

1. REISSUANCE AND PURPOSE
This Directive:
• Reissues Reference (a) and implements References (b), (c), and (d); section 188 of Public Law 108-458 (Reference (e)); Executive Order 12863 (Reference (f)); and chapter 36 of title 50, United States Code (Reference (g)).
• Updates policy and provides direction for DoD intelligence activities.
• Shall be the primary authority used as guidance by the Defense Intelligence Components and those performing an intelligence or
counterintelligence (CI) function to collect, process, retain, or disseminate information concerning U.S. persons.

- Continues to authorize the publication of DoD 5240.1-R (Reference (h)).

### 2. APPLICABILITY AND SCOPE

This Directive:

- 2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the “DoD Components”).

- 2.2. Applies to all intelligence activities conducted by the DoD Components.

- 2.3. Does not apply to authorized law enforcement activities carried out by the Defense Intelligence Components, or to individuals executing law enforcement missions while assigned to the Defense Intelligence Components.

### 3. DEFINITIONS

Terms used in this Directive are defined in Enclosure 2.

### 4. POLICY

It is DoD policy that:

- 4.1. All DoD intelligence and CI activities shall be carried out pursuant to the authorities and restrictions of the U.S. Constitution, applicable law, Reference (c), the policies and procedures authorized herein, and other relevant DoD policies authorized by Reference (b). Special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. persons.

- 4.2. DoD intelligence and CI activities shall conform to U.S. law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).

- 4.3. Defense Intelligence and CI shall be the all-source information collection, analysis, sharing, and dissemination capability derived from intelligence and CI activities, operations, and campaign plans, provided to national and defense decision makers and warfighters for military planning and operations.

- 4.4. Defense Intelligence shall provide accurate and timely warning of threats and of foreign capabilities and intent to national and defense decision makers to allow for consideration of the widest range of options.
While Defense Intelligence must be timely, it also must be substantive, thorough, contextual, and useful in form and format.

- 4.5. Consistent with the need to protect intelligence sources and methods and the provisions of Director of Central Intelligence Directive 8/1 (Reference (i)), the Defense Intelligence and CI Components have an affirmative responsibility to share collected and stored information, data, and resulting analysis with other Defense Intelligence and CI Components, the national Intelligence Community (IC), other relevant Federal agencies, and civilian law enforcement officials, as appropriate. This also applies to the exchange and sharing of terrorism-related information pursuant to Reference (d). Information sharing shall adhere to the requirements and restrictions imposed by Federal law, Executive order, and DoD and DNI policies.
  - 4.5.1. The Defense Intelligence and CI Components shall share collected or stored information in a manner consistent with both the need to protect sources and methods and the need to enable the Defense Intelligence and DoD Components, other Government agencies, and the Intelligence Community, as appropriate, to accomplish their missions and responsibilities.
  - 4.5.2. The broadest possible sharing of intelligence with coalition and approved partner countries shall be accomplished unless otherwise precluded from release by law, explicit direction, or policy.
  - 4.5.3. Original classifiers shall draft intelligence products with a presumption of release and in such a manner as to allow the widest dissemination to allies, coalitions, and international organizations.

- 4.6. No Defense Intelligence or CI Component shall request any person or entity to undertake unauthorized activities on behalf of the Defense Intelligence or CI Component. No Defense Intelligence or CI Component shall request any person or entity to undertake intelligence activities on behalf of the Defense Intelligence or CI Component that do not follow the procedures described in Reference (h). The collection techniques described in Reference (h) shall be employed only to perform intelligence or CI functions assigned to the Defense Intelligence Component concerned. Use of such techniques to collect information about U.S. persons shall be limited to the least intrusive means feasible and shall not violate law, Executive order, Presidential guidance, or DoD or DNI policy.

- 4.7. The Defense Intelligence and CI Components and their employees shall report all intelligence or CI activities that may violate law, Executive order, Presidential directive, or applicable DoD policy through the Component chain of command to the Inspector General or General Counsel responsible for the Defense Intelligence Component concerned, or to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)).
• 4.8. The Defense Intelligence Components shall only conduct, or provide support for the conduct of, covert activities in times of war declared by Congress, during a period covered by a report from the President to Congress consistent with sections 1541-1548 of Reference (g), or when such actions have been approved by the President and directed by the Secretary of Defense.

• 4.9. Under no circumstances shall any DoD Component or DoD employee engage in, or conspire to engage in, assassination.

5. RESPONSIBILITIES

• 5.1. The Under Secretary of Defense for Intelligence (USD(I)), according to Reference (b), shall provide overall policy guidance for the conduct of DoD intelligence, CI, security, and intelligence-related activities. Pursuant to Reference (b), the USD(I) shall:
  o 5.1.1. Serve as the focal point for the Secretary of Defense, according to the responsibilities and functions prescribed herein, with other U.S. Government entities and agencies, including the National Security Council, the DNI, the Homeland Security Council, the Department of the Treasury, the Department of State, the Department of Justice, and the Department of Homeland Security as well as State agencies, the IC, and Congress.
  o 5.1.2. Serve as the focal point for the Secretary of Defense, according to the responsibilities and functions prescribed herein, with foreign governments, international organizations, and non-governmental organizations.
  o 5.1.3. Promote coordination, cooperation, information sharing, and crossservice management of intelligence, CI, security, and related programs within the Department of Defense and between the Department and other Federal agencies.
  o 5.1.4. Provide oversight and policy guidance on sensitive intelligence activities; serve as the DoD lead for Departmental participation in all such activities.

• 5.2. The Department of Defense General Counsel shall:
  o 5.2.1. Serve as the focal point for contact with, and reporting to, the Attorney General regarding legal matters arising under this Directive.
  o 5.2.2. Interpret this Directive and Reference (h), as required.

• 5.3. The ATSD(IO) shall serve as the focal point for all contacts with the Intelligence Oversight Board of the President’s Foreign Intelligence Advisory Board pursuant to Reference (f), and shall perform the responsibilities assigned in DoD Directive 5148.11 (Reference (j)).

• 5.4. The Secretaries of the Military Departments with IC elements shall:
5.4.1. Organize, staff, train, and equip the intelligence assets of the Military Departments, including CI, signals intelligence, geospatial intelligence, measurement and signatures intelligence, and human intelligence assets, to support operational forces, national-level policy-makers, and the acquisition community.

5.4.2. Develop intelligence capabilities including interoperable and compatible systems, databases, and procedures for joint operational forces according to DoD guidance; Combatant Commander and Director, Defense Intelligence Agency, requirements; the Defense Intelligence Information System Network-Centric Architecture; and the Joint Technical Architecture.

5.4.3. Fulfill assigned Defense Intelligence Analysis Program responsibilities, both national level and Military Department-unique, for national intelligence activities in support of national and DoD entities through timely, tailored, all-source intelligence tasking, collection, processing/exploitation, analysis/production, and dissemination/integration.

6. EFFECTIVE DATE
This Directive is effective immediately.

Enclosures – 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1 - REFERENCES, continued

- (e) Section 188 of Public Law 108-458, “Intelligence Reform and Terrorism Prevention Act of 2004,” December 17, 2004
- (f) Executive Order 12863, “President’s Foreign Intelligence Advisory Board,” September 13, 1993, as amended by Executive Order 13070, December 15, 1997; Executive Order 13301, May 14, 2003; and Executive Order 13376, April 13, 2005
- (g) Chapter 36 and sections 401a(2), 413, and 1541-1548 of title 50, United State Code
- Director of Central Intelligence Directive 8/1, “Intelligence Community Policy on Intelligence Information Sharing,” June 4, 2004
- (j) DoD Directive 5148.11, “Assistant to the Secretary of Defense (Intelligence Oversight),” May 21, 2004
E2. ENCLOSURE 2 - DEFINITIONS
E2.1. All-Source Analysis
An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement and signature intelligence, and open source intelligence.

E2.2. CI
Defined in Joint Publication 1-02 (Reference (k)).

E2.3. Defense CI Components
Defined in Reference (b).

E2.4. Defense Intelligence
Defined in Reference (b).

E2.5. Defense Intelligence Components
Defined in Reference (b).

E2.6. Foreign Intelligence
Defined in section 401a(2) of Reference (g).

E2.7. Intelligence Activities
The collection, analysis, production, and dissemination of foreign intelligence and CI pursuant to References (b) and (c).

E2.8. National Intelligence
Defined in Reference (b).

E2.9. Covert Action
Defined in section 413 of Reference (g).

E2.10. U.S. Person
Defined in Reference (c).
The Attorney General’s Guidelines for Domestic FBI Operations

As Amended Through January 1, 2010

Table of Contents

- PREAMBLE
- INTRODUCTION
- I. GENERAL AUTHORITIES AND PRINCIPLES
- II. INVESTIGATIONS AND INTELLIGENCE GATHERING
- III. ASSISTANCE TO OTHER AGENCIES
- IV. INTELLIGENCE ANALYSIS AND PLANNING
- V. AUTHORIZED METHODS
- VI. RETENTION AND SHARING OF INFORMATION
- VII. DEFINITIONS

PREAMBLE
These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333. They apply to domestic investigative activities of the Federal Bureau of Investigation (FBI) and other activities as provided herein.

INTRODUCTION
As the primary investigative agency of the federal government, the Federal Bureau of Investigation (FBI) has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out investigations within the United States of threats to the national security. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to meet foreign entities’ espionage and intelligence efforts directed against the United States. The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the U.S. Intelligence Community. The FBI accordingly plays crucial roles in the
enforcement of federal law and the proper administration of justice in the United States, in the protection of the national security, and in obtaining information needed by the United States for the conduct of its foreign affairs. These roles reflect the wide range of the FBI's current responsibilities and obligations, which require the FBI to be both an agency that effectively detects, investigates, and prevents crimes, and an agency that effectively protects the national security and collects intelligence.

The general objective of these Guidelines is the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States. At the same time, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people. The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

The issuance of these Guidelines represents the culmination of the historical evolution of the FBI and the policies governing its domestic operations subsequent to the September 11, 2001, terrorist attacks on the United States. Reflecting decisions and directives of the President and the Attorney General, inquiries and enactments of Congress, and the conclusions of national commissions, it was recognized that the FBI's functions needed to be expanded and better integrated to meet contemporary realities:

[Continuing coordination . . . is necessary to optimize the FBI's performance in both national security and criminal investigations . . . . [The] new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very different FBI from the one we had on September 10,2001. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 466,452 (2005).)

In line with these objectives, the FBI has reorganized and reoriented its programs and missions, and the guidelines issued by the Attorney General for FBI operations have been extensively revised over the past several years. Nevertheless, the principal directives of the Attorney General governing the FBI's conduct of criminal investigations, national security investigations, and foreign
intelligence collection have persisted as separate documents involving different standards and procedures for comparable activities. These Guidelines effect a more complete integration and harmonization of standards, thereby providing the FBI and other affected Justice Department components with clearer, more consistent, and more accessible guidance for their activities, and making available to the public in a single document the basic body of rules for the FBI's domestic operations.

These Guidelines also incorporate effective oversight measures involving many Department of Justice and FBI components, which have been adopted to ensure that all FBI activities are conducted in a manner consistent with law and policy.

The broad operational areas addressed by these Guidelines are the FBI's conduct of investigative and intelligence gathering activities, including cooperation and coordination with other components and agencies in such activities, and the intelligence analysis and planning functions of the FBI.

A. FBI RESPONSIBILITIES—FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE

Part 110f these Guidelines authorizes the FBI to carry out investigations to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. The major subject areas of information gathering activities under these Guidelines—federal crimes, threats to the national security, and foreign intelligence—are not distinct, but rather overlap extensively. For example, an investigation relating to international terrorism will invariably crosscut these areas because international terrorism is included under these Guidelines' definition of "threat to the national security," because international terrorism subject to investigation within the United States usually involves criminal acts that violate federal law, and because information relating to international terrorism also falls within the definition of "foreign intelligence." Likewise, counterintelligence activities relating to espionage are likely to concern matters that constitute threats to the national security, that implicate violations or potential violations of federal espionage laws, and that involve information falling under the definition of "foreign intelligence."

While some distinctions in the requirements and procedures for investigations are necessary in different subject areas, the general design of these Guidelines is to take a uniform approach wherever possible, thereby promoting certainty and consistency regarding the applicable standards and facilitating compliance with those standards. Hence, these Guidelines do not require that the FBI's information gathering activities be differentially labeled as "criminal investigations," "national security investigations," or "foreign intelligence collections," or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI's legal authorities are available for deployment in all cases.
to which they apply to protect the public from crimes and threats to the national security and to further the United States’ foreign intelligence objectives. In many cases, a single investigation will be supportable as an exercise of a number of these authorities - i.e., as an investigation of a federal crime or crimes, as an investigation of a threat to the national security, and/or as a collection of foreign intelligence.

1. Federal Crimes
The FBI has the authority to investigate all federal crimes that are not exclusively assigned to other agencies. In most ordinary criminal investigations, the immediate objectives include such matters as: determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; and obtaining the evidence needed for prosecution. Hence, close cooperation and coordination with federal prosecutors in the United States Attorneys’ Offices and the Justice Department litigating divisions are essential both to ensure that agents have the investigative tools and legal advice at their disposal for which prosecutorial assistance or approval is needed, and to ensure that investigations are conducted in a manner that will lead to successful prosecution. Provisions in many parts of these Guidelines establish procedures and requirements for such coordination.

2. Threats to the National Security
The FBI’s authority to investigate threats to the national security derives from the executive order concerning U.S. intelligence activities, from delegations of functions by the Attorney General, and from various statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq. These Guidelines (Part VII.S) specifically define threats to the national security to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order. Activities within the definition of "threat to the national security" that are subject to investigation under these Guidelines commonly involve violations (or potential violations) of federal criminal laws. Hence, investigations of such threats may constitute an exercise both of the FBI’s criminal investigation authority and of the FBI's authority to investigate threats to the national security. As with criminal investigations generally, detecting and solving the crimes, and eventually arresting and prosecuting the perpetrators, are likely to be among the objectives of investigations relating to threats to the national security. But these investigations also often serve important purposes outside the ambit of normal criminal investigation and prosecution, by providing the basis for, and informing decisions concerning, other measures needed to protect the national security. These measures may include, for example: excluding or removing persons involved in terrorism or espionage from the United States; recruitment of double
agents; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats.

In line with this broad range of purposes, investigations of threats to the national security present special needs to coordinate with other Justice Department components, including particularly the Justice Department's National Security Division, and to share information and cooperate with other agencies with national security responsibilities, including other agencies of the U.S. Intelligence Community, the Department of Homeland Security, and relevant White House (including National Security Council and Homeland Security Council) agencies and entities. Various provisions in these Guidelines establish procedures and requirements to facilitate such coordination.

3. Foreign Intelligence
As with the investigation of threats to the national security, the FBI's authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq.; 28 U.S.C. 532 note (incorporating P.L. 108-458 §5 2001-2003). These Guidelines (Part VII.E) define foreign intelligence to mean "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists."

The FBI's foreign intelligence collection activities have been expanded by legislative and administrative reforms subsequent to the September 11, 2001, terrorist attacks, reflecting the FBI's role as the primary collector of foreign intelligence within the United States, and the recognized imperative that the United States' foreign intelligence collection activities become more flexible, more proactive, and more efficient in order to protect the homeland and adequately inform the United States' crucial decisions in its dealings with the rest of the world:

The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect information . . . turns analysis into guesswork. And as our review demonstrates, the Intelligence Community's human and technical intelligence collection agencies have collected far too little information on many of the issues we care about most. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 351 (2005).)
These Guidelines accordingly provide standards and procedures for the FBI's foreign intelligence collection activities that meet current needs and realities and optimize the FBI's ability to discharge its foreign intelligence collection functions.

The authority to collect foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security, and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. The FBI's role is central to the effective collection of foreign intelligence within the United States because the authorized domestic activities of other intelligence agencies are more constrained than those of the FBI under applicable statutes and Executive Order 12333. In collecting foreign intelligence, the FBI will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives issued under the authority of the Director of National Intelligence (DNI). As provided in Part VII.F of these Guidelines, foreign intelligence requirements may also be established by the President or Intelligence Community officials designated by the President, and by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

The general guidance of the FBI's foreign intelligence collection activities by DNI-authorized requirements does not, however, limit the FBI's authority to conduct investigations supportable on the basis of its other authorities to investigate federal crimes and threats to the national security in areas in which the information sought also falls under the definition of foreign intelligence. The FBI conducts investigations of federal crimes and threats to the national security based on priorities and strategic objectives set by the Department of Justice and the FBI, independent of DNI-established foreign intelligence collection requirements.

Since the authority to collect foreign intelligence enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information so gathered may concern lawful activities. The FBI should accordingly operate openly and consensually with U.S. persons to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

B. THE FBI AS AN INTELLIGENCE AGENCY
The FBI is an intelligence agency as well as a law enforcement agency. Its basic functions accordingly extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See, e.g., E.O.
12333; 28 U.S.C. 532 note (incorporating P.L. 108-458 §5 2001 -2003) and 534 note (incorporating P.L. 109-1 62 8 1 107). Enhancement of the FBI's intelligence analysis capabilities and functions has consistently been recognized as a key priority in the legislative and administrative reform efforts following the September 11,2001, terrorist attacks:

[Counterterrorism] strategy should . . . encompass specific efforts to . . . enhance the depth and quality of domestic intelligence collection and analysis . . . . [T]he FBI should strengthen and improve its domestic [intelligence] capability as fully and expeditiously as possible by immediately instituting measures to . . . significantly improve strategic analytical capabilities . . . . (Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11,2001, S. Rep. No. 351 & H.R. Rep. No. 792, 107th Cong., 2d Sess. 4-7 (2002) (errata print).)

A "smart" government would integrate all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence. . . . The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." (Final Report of the National Commission on Terrorist Attacks Upon the United States 401,408 (2004).)

Part IV of these Guidelines accordingly authorizes the FBI to engage in intelligence analysis and planning, drawing on all lawful sources of information. The functions authorized under that Part include: (i) development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, (ii) research and analysis to produce reports and assessments concerning matters relevant to investigative activities or other authorized FBI activities, and (iii) the operation of intelligence systems that facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis.

C. OVERSIGHT
The activities authorized by these Guidelines must be conducted in a manner consistent with all applicable laws, regulations, and policies, including those protecting privacy and civil liberties. The Justice Department's National Security Division and the FBI's Inspection Division, Office of General Counsel, and Office of Integrity and Compliance, along with other components, share the responsibility to ensure that the Department meets these goals with respect to national security and foreign intelligence matters. In particular, the National Security Division's Oversight Section, in conjunction with the FBI's Office of General Counsel, is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. These reviews, conducted
at FBI field offices and headquarter units, broadly examine such activities for
compliance with these Guidelines and other applicable requirements.

Various features of these Guidelines facilitate the National Security Division's
oversight functions. Relevant requirements and provisions include: (i) required
notification by the FBI to the National Security Division concerning full
investigations that involve foreign intelligence collection or investigation of
United States persons in relation to threats of the national security,
(ii) annual reports by the FBI to the National Security Division concerning the
FBI's foreign intelligence collection program, including information on the scope
and nature of foreign intelligence collection activities in each FBI field office, and
(iii) access by the National Security Division to information obtained by the FBI
through national security or foreign intelligence activities and general authority
for the Assistant Attorney General for National Security to obtain reports from
the FBI concerning these activities.

Pursuant to these Guidelines, other Attorney General guidelines, and
institutional assignments of responsibility within the Justice Department,
additional Department components—including the Criminal Division, the United
States Attorneys' Offices, and the Office of Privacy and Civil Liberties—are
involved in the common endeavor with the FBI of ensuring that the activities of
all Department components are lawful, appropriate, and ethical as well as
effective. Examples include the involvement of both FBI and prosecutorial
personnel in the review of undercover operations involving sensitive
circumstances, notice requirements for investigations involving sensitive
investigative matters (as defined in Part V11.N of these Guidelines), and notice
and oversight provisions for enterprise investigations, which may involve a broad
examination of groups implicated in the gravest criminal and national security
threats. These requirements and procedures help to ensure that the rule of law is
respected in the Department's activities and that public confidence is maintained
in these activities.
I. GENERAL AUTHORITIES AND PRINCIPLES

A. SCOPE
These Guidelines apply to investigative activities conducted by the FBI within the United States or outside the territories of all countries. They do not apply to investigative activities of the FBI in foreign countries, which are governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

B. GENERAL AUTHORITIES
1. The FBI is authorized to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in Part II of these Guidelines.
2. The FBI is authorized to provide investigative assistance to other federal agencies, state, local, or tribal agencies, and foreign agencies as provided in Part III of these Guidelines.
3. The FBI is authorized to conduct intelligence analysis and planning as provided in Part IV of these Guidelines.
4. The FBI is authorized to retain and share information obtained pursuant to these Guidelines as provided in Part VI of these Guidelines.

C. USE OF AUTHORITIES AND METHODS
1. Protection of the United States and Its People
The FBI shall fully utilize the authorities provided and the methods authorized by these Guidelines to protect the United States and its people from crimes in violation of federal law and threats to the national security, and to further the foreign intelligence objectives of the United States.

2. Choice of Methods
a. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized, however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.
b. United States persons shall be dealt with openly and consensually to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

3. Respect for Legal Rights
All activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines. These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. These Guidelines also do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies.

4. Undisclosed Participation in Organizations
Undisclosed participation in organizations in activities under these Guidelines shall be conducted in accordance with FBI policy approved by the Attorney General.

5. Maintenance of Records under the Privacy Act
The Privacy Act restricts the maintenance of records relating to certain activities of individuals who are United States persons, with exceptions for circumstances in which the collection of such information is pertinent to and within the scope of an authorized law enforcement activity or is otherwise authorized by statute. 5 U.S.C. 552a(e)(7). Activities authorized by these Guidelines are authorized law enforcement activities or activities for which there is otherwise statutory authority for purposes of the Privacy Act. These Guidelines, however, do not provide an exhaustive enumeration of authorized FBI law enforcement activities or FBI activities for which there is otherwise statutory authority, and no restriction is implied with respect to such activities carried out by the FBI pursuant to other authorities. Further questions about the application of the Privacy Act to authorized activities of the FBI should be addressed to the FBI Office of the General Counsel, the FBI Privacy and Civil Liberties Unit, or the Department of Justice Office of Privacy and Civil Liberties.

D. NATURE AND APPLICATION OF THE GUIDELINES
1. Repealers
These Guidelines supersed the following guidelines, which are hereby repealed:
   b. The Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) and all predecessor guidelines thereto.
c. The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006).

d. The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988).


2. Status as Internal Guidance

These Guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice.

3. Departures from the Guidelines

Departures from these Guidelines must be approved by the Director of the FBI, by the Deputy Director of the FBI, or by an Executive Assistant Director designated by the Director. If a departure is necessary without such prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director, the Deputy Director, or a designated Executive Assistant Director shall be notified as soon thereafter as practicable. The FBI shall provide timely written notice of departures from these Guidelines to the Criminal Division and the National Security Division, and those divisions shall notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

4. Other Activities Not Limited

These Guidelines apply to FBI activities as provided herein and do not limit other authorized activities of the FBI, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory.
II. INVESTIGATIONS AND INTELLIGENCE GATHERING

This Part of the Guidelines authorizes the FBI to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence.

When an authorized purpose exists, the focus of activities authorized by this Part may be whatever the circumstances warrant. The subject of such an activity may be, for example, a particular crime or threatened crime; conduct constituting a threat to the national security; an individual, group, or organization that may be involved in criminal or national security-threatening conduct; or a topical matter of foreign intelligence interest.

Investigations may also be undertaken for protective purposes in relation to individuals, groups, or other entities that may be targeted for criminal victimization or acquisition, or for terrorist attack or other depredations by the enemies of the United States. For example, the participation of the FBI in special events management, in relation to public events or other activities whose character may make them attractive targets for terrorist attack, is an authorized exercise of the authorities conveyed by these Guidelines. Likewise, FBI counterintelligence activities directed to identifying and securing facilities, personnel, or information that may be targeted for infiltration, recruitment, or acquisition by foreign intelligence services are authorized exercises of the authorities conveyed by these Guidelines.

The identification and recruitment of human sources—who may be able to provide or obtain information relating to criminal activities, information relating to terrorism, espionage, or other threats to the national security, or information relating to matters of foreign intelligence interest—is also critical to the effectiveness of the FBI’s law enforcement, national security, and intelligence programs, and activities undertaken for this purpose are authorized and encouraged.

The scope of authorized activities under this Part is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under Part IV, and dissemination of the information to other law enforcement, Intelligence Community, and White House agencies under Part VI. Information obtained at all stages of investigative activity is accordingly to be retained and disseminated for these purposes as
provided in these Guidelines, or in FBI policy consistent with these Guidelines, regardless of whether it furthers investigative objectives in a narrower or more immediate sense.

In the course of activities under these Guidelines, the FBI may incidentally obtain information relating to matters outside of its areas of primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. These Guidelines do not bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other agencies or jurisdictions. Part VI of these Guidelines includes specific authorizations and requirements for sharing such information with relevant agencies and officials.

This Part authorizes different levels of information gathering activity, which afford the FBI flexibility, under appropriate standards and procedures, to adapt the methods utilized and the information sought to the nature of the matter under investigation and the character of the information supporting the need for investigation.

Assessments, authorized by Subpart A of this Part, require an authorized purpose but not any particular factual predication. For example, to carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity, or facility has drawn the attention of those who would threaten the national security. Rather, the FBI must take the initiative to secure and protect activities and entities whose character may make them attractive targets for terrorism or espionage. The proactive investigative authority conveyed in assessments is designed for, and may be utilized by, the FBI in the discharge of these responsibilities. For example, assessments may be conducted as part of the FBI's special events management activities.

More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots and activities to come to fruition. Hence, assessments may be undertaken proactively with such objectives as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or
victimization by such activities; and identifying and assessing individuals who may have value as human sources. For example, assessment activities may involve proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place; through which child pornography is advertised and traded; through which efforts are made by sexual predators to lure children for purposes of sexual abuse; or through which fraudulent schemes are perpetrated against the public.

The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly available information, checking government records, and requesting information from members of the public. These Guidelines do not impose supervisory approval requirements in assessments, given the types of techniques that are authorized at this stage (e.g., perusing the Internet for publicly available information). However, FBI policy will prescribe supervisory approval requirements for certain assessments, considering such matters as the purpose of the assessment and the methods being utilized.

Beyond the proactive information gathering functions described above, assessments may be used when allegations or other information concerning crimes or threats to the national security is received or obtained, and the matter can be checked out or resolved through the relatively non-intrusive methods authorized in assessments. The checking of investigative leads in this manner can avoid the need to proceed to more formal levels of investigative activity, if the results of an assessment indicate that further investigation is not warranted.

Subpart B of this Part authorizes a second level of investigative activity, predicated investigations. The purposes or objectives of predicated investigations are essentially the same as those of assessments, but predication as provided in these Guidelines is needed—generally, allegations, reports, facts or circumstances indicative of possible criminal or national security-threatening activity, or the potential for acquiring information responsive to foreign intelligence requirements—and supervisory approval must be obtained, to initiate predicated investigations. Corresponding to the stronger predication and approval requirements, all lawful methods may be used in predicated investigations. A classified directive provides further specification concerning circumstances supporting certain predicated investigations.

Predicated investigations that concern federal crimes or threats to the national security are subdivided into preliminary investigations and full investigations. Preliminary investigations may be initiated on the basis of any allegation or information indicative of possible criminal or national security-threatening activity, but more substantial factual predication is required for full investigations. While time limits are set for the completion of preliminary
investigations, full investigations may be pursued without preset limits on their duration.

The final investigative category under this Part of the Guidelines is enterprise investigations, authorized by Subpart C, which permit a general examination of the structure, scope, and nature of certain groups and organizations. Enterprise investigations are a type of full investigations. Hence, they are subject to the purpose, approval, and predication requirements that apply to full investigations, and all lawful methods may be used in carrying them out. The distinctive characteristic of enterprise investigations is that they concern groups or organizations that may be involved in the most serious criminal or national security threats to the public - generally, patterns of racketeering activity, terrorism or other threats to the national security, or the commission of offenses characteristically involved in terrorism as described in 18 U.S.C. 2332b(g)(5)(B). A broad examination of the characteristics of groups satisfying these criteria is authorized in enterprise investigations, including any relationship of the group to a foreign power, its size and composition, its geographic dimensions and finances, its past acts and goals, and its capacity for harm.

A. ASSESSMENTS

1. Purposes
Assessments may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval
The conduct of assessments is subject to any supervisory approval requirements prescribed by FBI policy.

3. Authorized Activities
Activities that may be carried out for the purposes described in paragraph 1 in an assessment include:
   a. seeking information, proactively or in response to investigative leads, relating to:
      i. activities constituting violations of federal criminal law or threats to the national security,
      ii. the involvement or role of individuals, groups, or organizations in such activities; or
      iii. matters of foreign intelligence interest responsive to foreign intelligence requirements;
   b. identifying and obtaining information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security;
   c. seeking information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate
human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and
d. obtaining information to inform or facilitate intelligence analysis and planning as described in Part IV of these Guidelines.

4. Authorized Methods
Only the following methods may be used in assessments:

a. Obtain publicly available information.
b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
d. Use online services and resources (whether nonprofit or commercial).
e. Use and recruit human sources in conformity with the Attorney General’s Guidelines Regarding the Use of FBI Confidential Human Sources.
f. Interview or request information from members of the public and private entities.
g. Accept information voluntarily provided by governmental or private entities.
h. Engage in observation or surveillance not requiring a court order.
i. Grand jury subpoenas for telephone or electronic mail subscriber information.

B. PREDICATED INVESTIGATIONS

1. Purposes
Predicated investigations may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval
The initiation of a predicated investigation requires supervisory approval at a level or levels specified by FBI policy. A predicated investigation based on paragraph 3.c. (relating to foreign intelligence) must be approved by a Special Agent in Charge or by an FBI Headquarters official as provided in such policy.

3. Circumstances Warranting Investigation
A predicated investigation may be initiated on the basis of any of the following circumstances:
a. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the
activity or the involvement or role of an individual, group, or organization in such activity.

b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat.

c. The investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.

4. Preliminary and Full Investigations
A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based solely on the authority to collect foreign intelligence may be conducted only as a full investigation.

a. Preliminary investigations

i. Predication Required for Preliminary Investigations
A preliminary investigation may be initiated on the basis of information or an allegation indicating the existence of a circumstance described in paragraph 3.a.-b.

ii. Duration of Preliminary Investigations
A preliminary investigation must be concluded within six months of its initiation, which may be extended by up to six months by the Special Agent in Charge. Extensions of preliminary investigations beyond a year must be approved by FBI Headquarters.

iii. Methods Allowed in Preliminary Investigations
All lawful methods may be used in a preliminary investigation except for methods within the scope of Part V.A. 11.--.13. of these Guidelines.

b. Full Investigations

i. Predication Required for Full Investigations
A full investigation may be initiated if there is an articulable factual basis for the investigation that reasonably indicates that a circumstance described in paragraph 3.a.-b. exists or if a circumstance described in paragraph 3.c. exists.

ii. Methods Allowed in Full Investigations
All lawful methods may be used in a full investigation.

5. Notice Requirements
a. An FBI field office shall notify FBI Headquarters and the United States Attorney or other appropriate Department of Justice official of the initiation by the field office of a predicated investigation involving a
sensitive investigative matter. If the investigation is initiated by FBI Headquarters, FBI Headquarters shall notify the United States Attorney or other appropriate Department of Justice official of the initiation of such an investigation. If the investigation concerns a threat to the national security, an official of the National Security Division must be notified. The notice shall identify all sensitive investigative matters involved in the investigation.

b. The FBI shall notify the National Security Division of:
   i. the initiation of any full investigation of a United States person relating to a threat to the national security; and
   ii. the initiation of any full investigation that is based on paragraph 3.c. (relating to foreign intelligence).

c. The notifications under subparagraphs a. and b. shall be made as soon as practicable, but no later than 30 days after the initiation of an investigation.

d. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a predicated investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient.

**C. ENTERPRISE INVESTIGATIONS**

1. Definition
   A full investigation of a group or organization may be initiated as an enterprise investigation if there is an articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:
   a. a pattern of racketeering activity as defined in 18 U.S.C. 1961 (5);
   b. international terrorism or other threat to the national security;
   c. domestic terrorism as defined in 18 U.S.C. 2331(5) involving a violation of federal criminal law;
   d. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
   e. an offense described in 18 U.S.C. 2332b(g)(5)(B) or 18 U.S.C. 43.

2. Scope
   The information sought in an enterprise investigation may include a general examination of the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; and its past and future activities and goals.

3. Notice and Reporting Requirements
a. The responsible Department of Justice component for the purpose of notification and reports in enterprise investigations is the National Security Division, except that, for the purpose of notifications and reports in an enterprise investigation relating to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the responsible Department of Justice component is the Organized Crime and Racketeering Section of the Criminal Division.

b. An FBI field office shall notify FBI Headquarters of the initiation by the field office of an enterprise investigation.

c. The FBI shall notify the National Security Division or the Organized Crime and Racketeering Section of the initiation of an enterprise investigation, whether by a field office or by FBI Headquarters, and the component so notified shall notify the Attorney General and the Deputy Attorney General. The FBI shall also notify any relevant United States Attorney's Office, except that any investigation within the scope of Part V1.D.1.d of these Guidelines (relating to counterintelligence investigations) is to be treated as provided in that provision. Notifications by the FBI under this subparagraph shall be provided as soon as practicable, but no later than 30 days after the initiation of the investigation.

d. The Assistant Attorney General for National Security or the Chief of the Organized Crime and Racketeering Section, as appropriate, may at any time request the FBI to provide a report on the status of an enterprise investigation and the FBI will provide such reports as requested.
III. ASSISTANCE TO OTHER AGENCIES

The FBI is authorized to provide investigative assistance to other federal, state, local, or tribal, or foreign agencies as provided in this Part.

The investigative assistance authorized by this Part is often concerned with the same objectives as those identified in Part II of these Guidelines—investigating federal crimes and threats to the national security, and collecting foreign intelligence. In some cases, however, investigative assistance to other agencies is legally authorized for purposes other than those identified in Part II, such as assistance in certain contexts to state or local agencies in the investigation of crimes under state or local law, see 28 U.S.C. 540, 540A, 540B, and assistance to foreign agencies in the investigation of foreign law violations pursuant to international agreements. Investigative assistance for such legally authorized purposes is permitted under this Part, even if it is not for purposes identified as grounds for investigation under Part II.

The authorities provided by this Part are cumulative to Part II and do not limit the FBI's investigative activities under Part II. For example, Subpart B.2 in this Part authorizes investigative activities by the FBI in certain circumstances to inform decisions by the President concerning the deployment of troops to deal with civil disorders, and Subpart B.3 authorizes investigative activities to facilitate demonstrations and related public health and safety measures. The requirements and limitations in these provisions for conducting investigations for the specified purposes do not limit the FBI's authority under Part II to investigate federal crimes or threats to the national security that occur in the context of or in connection with civil disorders or demonstrations.

A. THE INTELLIGENCE COMMUNITY
The FBI may provide investigative assistance (including operational support) to authorized intelligence activities of other Intelligence Community agencies.

B. FEDERAL AGENCIES GENERALLY
1. In General
The FBI may provide assistance to any federal agency in the investigation of federal crimes or threats to the national security or in the collection of foreign intelligence, and investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the Secret Service in support of its protective responsibilities.

2. The President in Relation to Civil Disorders
a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as:
   i. The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area.
   ii. The potential for violence.
   iii. The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder.
   iv. The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders.
   v. The extent of state or local resources available to handle the disorder.

b. Investigations under this paragraph will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.

c. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.--d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

3. Public Health and Safety Authorities in Relation to Demonstrations

a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:
   i. The time, place, and type of activities planned.
   ii. The number of persons expected to participate.
   iii. The expected means and routes of travel for participants and expected time of arrival.
   iv. Any plans for lodging or housing of participants in connection with the demonstration.
b. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.-d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

C. STATE, LOCAL, OR TRIBAL AGENCIES
The FBI may provide investigative assistance to state, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to the national security, or for such other purposes as may be legally authorized.

D. FOREIGN AGENCIES
1. At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any United States person. Investigations or assistance under this paragraph must be approved as provided by FBI policy. The FBI shall notify the National Security Division concerning investigation or assistance under this paragraph where: (i) FBI Headquarters approval for the activity is required pursuant to the approval policy adopted by the FBI for purposes of this paragraph, and (ii) the activity relates to a threat to the national security. Notification to the National Security Division shall be made as soon as practicable but no later than 30 days after the approval. Provisions regarding notification to or coordination with the Central Intelligence Agency by the FBI in memoranda of understanding or agreements with the Central Intelligence Agency may also apply to activities under this paragraph.

2. The FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the United States unless such officers have provided prior notification to the Attorney General as required by 18 U.S.C. 951.

3. The FBI may conduct background inquiries concerning consenting individuals when requested by foreign government agencies.

4. The FBI may provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law.

E. APPLICABLE STANDARDS AND PROCEDURES
1. Authorized investigative assistance by the FBI to other agencies under this Part includes joint operations and activities with such agencies.

2. All lawful methods may be used in investigative assistance activities under this Part.
3. Where the methods used in investigative assistance activities under this Part go beyond the methods authorized in assessments under Part II.A.4 of these Guidelines, the following apply:

a. Supervisory approval must be obtained for the activity at a level or levels specified in FBI policy.

b. Notice must be provided concerning sensitive investigative matters in the manner described in Part II.B.5.

c. A database or records system must be maintained that permits, with respect to each such activity, the prompt retrieval of the status of the activity (open or closed), the dates of opening and closing, and the basis for the activity. This database or records system may be combined with the database or records system for predicated investigations required by Part VI.A.2.
IV. INTELLIGENCE ANALYSIS AND PLANNING

The FBI is authorized to engage in analysis and planning. The FBI’s analytic activities enable the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and strategic planning, the FBI can more effectively discover crimes, threats to the national security, and other matters of national intelligence interest and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities. For example, analysis of threats in the context of special events management, concerning public events or activities that may be targeted for terrorist attack, is an authorized activity under this Part.

In carrying out its intelligence functions under this Part, the FBI is authorized to draw on all lawful sources of information, including but not limited to the results of investigative activities under these Guidelines. Investigative activities under these Guidelines and other legally authorized activities through which the FBI acquires information, data, or intelligence may properly be utilized, structured, and prioritized so as to support and effectuate the FBI’s intelligence mission. The remainder of this Part provides further specification concerning activities and functions authorized as part of that mission.

A. STRATEGIC INTELLIGENCE ANALYSIS
The FBI is authorized to develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI's responsibilities, including domestic and international criminal threats and activities; domestic and international activities, circumstances, and developments affecting the national security; and matters relevant to the conduct of the United States' foreign affairs. The overviews and analyses prepared under this Subpart may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them.

B. REPORTS AND ASSESSMENTS GENERALLY
The FBI is authorized to conduct research, analyze information, and prepare reports and assessments concerning matters relevant to authorized FBI activities, such as reports and assessments concerning: types of criminals or criminal activities; organized crime groups; terrorism, espionage, or other threats to the national security; foreign intelligence matters; or the scope and nature of criminal activity in particular geographic areas or sectors of the economy.
C. INTELLIGENCE SYSTEMS
The FBI is authorized to operate intelligence, identification, tracking, and information systems in support of authorized investigative activities, or for such other or additional purposes as may be legally authorized, such as intelligence and tracking systems relating to terrorists, gangs, or organized crime groups.
V. AUTHORIZED METHODS

A. PARTICULAR METHODS

All lawful investigative methods may be used in activities under these Guidelines as authorized by these Guidelines. Authorized methods include, but are not limited to, those identified in the following list. The methods identified in the list are in some instances subject to special restrictions or review or approval requirements as noted:

1. The methods described in Part II.A.4 of these Guidelines.
2. Mail covers.
3. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers).
4. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. Where a sensitive monitoring circumstance is involved, the monitoring must be approved by the Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the National Security Division.
5. Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. (The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)
6. Polygraph examinations.
7. Undercover operations. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover operations must be carried out in conformity with the Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations. In investigations that are not subject to the preceding sentence because they concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the National Security Division in the review process.


11. Electronic surveillance in conformity with chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522), the Foreign Intelligence Surveillance Act, or Executive Order 12333 5 2.5.

12. Physical searches, including mail openings, in conformity with Rule 41 of the Federal Rules of Criminal Procedure, the Foreign Intelligence Surveillance Act, or Executive Order 12333 5 2.5. A classified directive provides additional limitation on certain searches.

13. Acquisition of foreign intelligence information in conformity with title VII of the Foreign Intelligence Surveillance Act.

B. SPECIAL REQUIREMENTS

Beyond the limitations noted in the list above relating to particular investigative methods, the following requirements are to be observed:

1. Contacts with Represented Persons

Contact with represented persons may implicate legal restrictions and affect the admissibility of resulting evidence. Hence, if an individual is known to be represented by counsel in a particular matter, the FBI will follow applicable law and Department procedure concerning contact with represented individuals in the absence of prior notice to counsel. The Special Agent in Charge and the United States Attorney or their designees shall consult periodically on applicable law and Department procedure. Where issues arise concerning the consistency of contacts with represented persons with applicable attorney conduct rules, the United States Attorney’s Office should consult with the Professional Responsibility Advisory Office.

2. Use of Classified Investigative Technologies

Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases.

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General’s Guidelines.
on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.

2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General’s Guidelines Regarding the Use of FBI Confidential Human Sources.

3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1 must be approved by a United States Attorney’s Office or a Department of Justice Division, except that a Special Agent in Charge may authorize the following:
   a. otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
   b. consensual monitoring of communications, even if a crime under state, local, or tribal law;
   c. the controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
   d. the payment of bribes;
   e. the making of false representations in concealment of personal identity or the true ownership of a proprietary; and
   f. conducting a money laundering transaction or transactions involving an aggregate amount not exceeding $1 million.

   However, in an investigation relating to a threat to the national security or foreign intelligence collection, a Special Agent in Charge may not authorize an activity that may constitute a violation of export control laws or laws that concern the proliferation of weapons of mass destruction. In such an investigation, a Special Agent in Charge may authorize an activity that may otherwise violate prohibitions of material support to terrorism only in accordance with standards established by the Director of the FBI and agreed to by the Assistant Attorney General for National Security.

4. The following activities may not be authorized:
   b. Activities whose authorization is prohibited by law, including unlawful investigative methods, such as illegal electronic surveillance or illegal searches.

   Subparagraph a., however, does not limit the right of FBI agents or employees to engage in any lawful use of force, including the use of force in self-defense or defense of others or otherwise in the lawful discharge of their duties.

5. An agent or employee may engage in otherwise illegal activity that could be authorized under this Subpart without the authorization required by paragraph 3 if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant
investigative opportunity. In such a case, prior to engaging in the otherwise illegal activity, every effort should be made by the agent or employee to consult with the Special Agent in Charge, and by the Special Agent in Charge to consult with the United States Attorney’s Office or appropriate Department of Justice Division where the authorization of that office or division would be required under paragraph 3., unless the circumstances preclude such consultation. Cases in which otherwise illegal activity occurs pursuant to this paragraph without the authorization required by paragraph 3 shall be reported as soon as possible to the Special Agent in Charge, and by the Special Agent in Charge to FBI Headquarters and to the United States Attorney’s Office or appropriate Department of Justice Division.

6. In an investigation relating to a threat to the national security or foreign intelligence collection, the National Security Division is the approving component for otherwise illegal activity for which paragraph 3 requires approval beyond internal FBI approval. However, officials in other components may approve otherwise illegal activity in such investigations as authorized by the Assistant Attorney General for National Security.
VI. RETENTION AND SHARING OF INFORMATION

A. RETENTION OF INFORMATION
1. The FBI shall retain records relating to activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration.
2. The FBI shall maintain a database or records system that permits, with respect to each predicated investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation.

B. INFORMATION SHARING GENERALLY
1. Permissive Sharing
Consistent with law and with any applicable agreements or understandings with other agencies concerning the dissemination of information they have provided, the FBI may disseminate information obtained or produced through activities under these Guidelines:
   a. within the FBI and to other components of the Department of Justice;
   b. to other federal, state, local, or tribal agencies if related to their responsibilities and, in relation to other Intelligence Community agencies, the determination whether the information is related to the recipient's responsibilities may be left to the recipient;
   c. to congressional committees as authorized by the Department of Justice Office of Legislative Affairs;
   d. to foreign agencies if the information is related to their responsibilities and the dissemination is consistent with the interests of the United States (including national security interests) and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person;
   e. if the information is publicly available, does not identify United States persons, or is disseminated with the consent of the person whom it concerns;
   f. if the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation; or
   g. if dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. 552a).

2. Required Sharing
The FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives,
Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements.

C. INFORMATION RELATING TO CRIMINAL MATTERS

1. Coordination with Prosecutors
In an investigation relating to possible criminal activity in violation of federal law, the agent conducting the investigation shall maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the agent shall present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

2. Criminal Matters Outside FBI Jurisdiction
When credible information is received by an FBI field office concerning serious criminal activity not within the FBI's investigative jurisdiction, the field office shall promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except where disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a human source, interfere with a human source's cooperation, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then, whenever feasible, the FBI field office shall make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure shall be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI field office shall promptly notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. The FBI shall make periodic reports to the Deputy Attorney General on such nondisclosures and incomplete disclosures, in a form suitable to protect the identity of human sources.

3. Reporting of Criminal Activity
a. When it appears that an FBI agent or employee has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall notify the United States Attorney's Office or an appropriate Department of Justice Division. When it appears that a human source has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall proceed as provided in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources. When information concerning possible criminal activity by any other person appears in the course of an investigation under these Guidelines, the FBI shall initiate an investigation of the criminal activity if warranted, and shall proceed as provided in paragraph 1 or 2.
b. The reporting requirements under this paragraph relating to criminal activity by FBI agents or employees or human sources do not apply to otherwise illegal activity that is authorized in conformity with these Guidelines or other Attorney General guidelines or to minor traffic offenses.

**D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS**

The general principle reflected in current laws and policies is that there is a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. The FBI's responsibilities in this area include carrying out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and consultation with other Department of Justice components, and for provision of national security and foreign intelligence information to White House agencies, as provided in the ensuing paragraphs.

1. Department of Justice

   a. The National Security Division shall have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security shall consult concerning these activities whenever requested by either of them, and the FBI shall provide such reports and information concerning these activities as the Assistant Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may specially request under this subparagraph, the FBI shall provide annual reports to the National Security Division concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office.

   b. The FBI shall keep the National Security Division apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, which shall include regular consultations between the FBI and the National Security Division to exchange advice and information relevant to addressing such threats through criminal prosecution or other means.

   c. Subject to subparagraphs d. and e., relevant United States Attorneys' Offices shall have access to and shall receive information from the FBI

   1. Department of Justice

   a. The National Security Division shall have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security shall consult concerning these activities whenever requested by either of them, and the FBI shall provide such reports and information concerning these activities as the Assistant Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may specially request under this subparagraph, the FBI shall provide annual reports to the National Security Division concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office.

   b. The FBI shall keep the National Security Division apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, which shall include regular consultations between the FBI and the National Security Division to exchange advice and information relevant to addressing such threats through criminal prosecution or other means.

   c. Subject to subparagraphs d. and e., relevant United States Attorneys' Offices shall have access to and shall receive information from the FBI

   1. Department of Justice

   a. The National Security Division shall have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security shall consult concerning these activities whenever requested by either of them, and the FBI shall provide such reports and information concerning these activities as the Assistant Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may specially request under this subparagraph, the FBI shall provide annual reports to the National Security Division concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office.

   b. The FBI shall keep the National Security Division apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, which shall include regular consultations between the FBI and the National Security Division to exchange advice and information relevant to addressing such threats through criminal prosecution or other means.

   c. Subject to subparagraphs d. and e., relevant United States Attorneys' Offices shall have access to and shall receive information from the FBI
relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the National Security Division. The relevant United States Attorneys' Offices shall receive such access and information from the FBI field offices.

d. In a counterintelligence investigation -i.e., an investigation relating to a matter described in Part VII.S.2 of these Guidelines -the FBI's provision of information to and consultation with a United States Attorney's Office are subject to authorization by the National Security Division. In consultation with the Executive Office for United States Attorneys and the FBI, the National Security Division shall establish policies setting forth circumstances in which the FBI will consult with the National Security Division prior to informing relevant United States Attorneys' Offices about such an investigation. The policies established by the National Security Division under this subparagraph shall (among other things) provide that:

i. the National Security Division will, within 30 days, authorize the FBI to share with the United States Attorneys' Offices information relating to certain espionage investigations, as defined by the policies, unless such information is withheld because of substantial national security considerations; and

ii. the FBI may consult freely with United States Attorneys' Offices concerning investigations within the scope of this subparagraph during an emergency, so long as the National Security Division is notified of such consultation as soon as practical after the consultation.

e. Information shared with a United States Attorney's Office pursuant to subparagraph c. or d. shall be disclosed only to the United States Attorney or any Assistant United States Attorneys designated by the United States Attorney as points of contact to receive such information. The United States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from the Foreign Intelligence Surveillance Act, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information.

f. The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of human sources is governed by the relevant provisions of the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

2. White House
In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the National Security Council and its staff, the Homeland Security Council and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. The FBI accordingly may disseminate to the White House foreign intelligence and national security information obtained through activities under these Guidelines, subject to the following standards and procedures:

a. Requests to the FBI for such information from the White House shall be made through the National Security Council staff or Homeland Security Council staff including, but not limited to, the National Security Council Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President’s Intelligence Advisory Board or the Counsel to the President.

b. Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel.

c. Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but are not limited to:

   i. information concerning international terrorism;
   ii. information concerning activities of foreign intelligence services in the United States;
   iii. information indicative of imminent hostilities involving any foreign power;
   iv. information concerning potential cyber threats to the United States or its allies;
   v. information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
   vi. information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
   vii. information concerning foreign economic or foreign political matters that might have national security ramifications; and
   viii. information set forth in regularly published national intelligence requirements.
d. Communications by the FBI to the White House that relate to a national security matter and concern a litigation issue for a specific pending case must be made known to the Office of the Attorney General, the Office of the Deputy Attorney General, or the Office of the Associate Attorney General. White House policy may specially limit or prescribe the White House personnel who may request information concerning such issues from the FBI.

e. The limitations on dissemination of information by the FBI to the White House under these Guidelines do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450.

3. Special Statutory Requirements

a. Dissemination of information acquired under the Foreign Intelligence Surveillance Act is, to the extent provided in that Act, subject to minimization procedures and other requirements specified in that Act.

b. Information obtained through the use of National Security Letters under 15 U.S.C. 1681v may be disseminated in conformity with the general standards of this Part. Information obtained through the use of National Security Letters under other statutes may be disseminated in conformity with the general standards of this Part, subject to any applicable limitations in their governing statutory provisions: 12 U.S.C. 3414(a)(5)(B); 15 U.S.C. 1681u(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e).
VII. DEFINITIONS

A. CONSENSUAL MONITORING:
Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

B. EMPLOYEE:
An FBI employee or an employee of another agency working under the direction and control of the FBI.

C. FOR OR ON BEHALF OF A FOREIGN POWER:
The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in:
1. control or policy direction;
2. financial or material support; or
3. leadership, assignments, or discipline.

D. FOREIGN COMPUTER INTRUSION:
The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers.

E. FOREIGN INTELLIGENCE:
Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

F. FOREIGN INTELLIGENCE REQUIREMENTS:
1. national intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
2. requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
3. directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

G. FOREIGN POWER:
1. a foreign government or any component thereof, whether or not recognized by the United States;
2. a faction of a foreign nation or nations, not substantially composed of United States persons;
3. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
4. a group engaged in international terrorism or activities in preparation therefor;
5. a foreign-based political organization, not substantially composed of United States persons; or
6. an entity that is directed or controlled by a foreign government or governments.

**H. HUMAN SOURCE:**
A Confidential Human Source as defined in the Attorney General’s Guidelines Regarding the Use of FBI Confidential Human Sources.

**I. INTELLIGENCE ACTIVITIES:**
Any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

**J. INTERNATIONAL TERRORISM:**
Activities that:
1. involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction;
2. appear to be intended:
   i. to intimidate or coerce a civilian population;
   ii. to influence the policy of a government by intimidation or coercion; or
   iii. to affect the conduct of a government by assassination or kidnapping; and
3. occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

**K. PROPRTETARY:**
A sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties.

**L. PUBLICLY AVAILABLE:**
Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

Page 1344
M. RECORDS:
Any records, databases, files, indices, information systems, or other retained information.

N. SENSITIVE INVESTIGATIVE MATTER:
An investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials.

O. SENSITIVE MONITORING CIRCUMSTANCE:
1. investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
2. investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
3. a party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
4. the Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

P. SPECIAL AGENT IN CHARGE:
The Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

Q. SPECIAL EVENTS MANAGEMENT:
Planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

R. STATE, LOCAL, OR TRIBAL:
Any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.

S. THREAT TO THE NATIONAL SECURITY:
1. international terrorism;
2. espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons;
3. foreign computer intrusion; and
4. other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

T. UNITED STATES:
When used in a geographic sense, means all areas under the territorial sovereignty of the United States.

U. UNITED STATES PERSON:
Any of the following, but not including any association or corporation that is a foreign power as defined in Subpart G.1.-3.:
1. an individual who is a United States citizen or an alien lawfully admitted for permanent residence;
2. an unincorporated association substantially composed of individuals who are United States persons; or
3. a corporation incorporated in the United States.

In applying paragraph 2., if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of United States persons. If, however, the U.S.-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is substantially composed of United States persons. A classified directive provides further guidance concerning the determination of United States person status.

V. USE:
When used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

Date: 9/29/08
Michael B. Mukasey
Attorney General
Foreign Intelligence Surveillance Court Rules
As Amended Through June 1, 2010

Table of Contents

- I. Scope, Construction, and Amendment of Rules
- II. National Security Information
- III. Structure of the Court and Authority of Judges
- IV. Attorneys Authorized to Appear Before the Court
- V. Clerk's Office
- VI. Form and Filing of Applications for Court Orders
- VII. Hearings
- VIII. Orders
- IX. Sequestration or Destruction
- X. Appeals

I. Scope, Construction, and Amendment of Rules

Rule 1: Scope of Rules
These rules govern all proceedings in the Foreign Intelligence Surveillance Court (hereafter, "the Court"). Issues not addressed in these rules may be resolved under the Federal Rules of Criminal Procedure or the Federal Rules of Civil Procedure.

Rule 2: Amendment
Any amendment to these rules shall be prescribed and promulgated in accordance with 28 U.S.C. § 2071.

II. National Security Information

Rule 3:
In all matters, the Court and its staff shall comply with the security measures established pursuant to 50 U.S.C. §§ 1803(c) and 1822(e), as well as Executive Order 12958, "Classified National Security Information," as amended by
Executive Order 13292 (or its successor). Each member of the Court's staff must possess security clearances at a level commensurate to the individual's responsibilities.

III. Structure of the Court and Authority of Judges

Rule 4: Structure
(a) Composition: In accordance with 50 U.S.C. § 1803(a), the Court consists of those United States District Court Judges appointed by the Chief Justice of the United States.

(b) Presiding Judge: The Presiding Judge is the Judge so designated by the Chief Justice.

Rule 5: Authority of the Judges
(a) Scope of Authority: Each Judge of the Court may exercise the authority vested by the Foreign Intelligence Surveillance Act, as amended, 50 U.S.C. § 1801 et seq. ("the Act"), including the authority to issue an Order approving electronic surveillance or a physical search, and such other authority, consonant with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.

(b) Authority to Refer Matters: Except for matters involving a denial of an application for a Court Order, a Judge may refer any matter to another Judge of the Court with that Judge's consent. If a Judge directs the government to supplement an application, that Judge may direct the government to present the next renewal of that application to that Judge. If a matter is presented to a Judge whose tenure on the Court expires while the matter is pending, the Presiding Judge shall reassign the matter.

(c) Publication of Opinions: On request by a Judge, the Presiding Judge, after consulting with other Judges of the Court, may direct that an Opinion be published. Before publication, the Opinion must be reviewed by the Executive Branch and redacted, as necessary, to ensure that properly classified information is appropriately protected pursuant to Executive Order 12958 as amended by Executive Order 13292 (or its successor).

IV. Attorneys Authorized to Appear Before the Court

Rule 6: License and Other Requirements for Attorneys
An attorney may appear on a matter with the permission of the Judge before whom the matter is pending. An attorney who appears before the Court must be a
licensed attorney and a member, in good standing, of the bar of a federal court, except that an attorney who is employed by and represents the United States or any of its agencies in a matter before the Court may appear before the Court regardless of federal bar membership. All attorneys appearing before the Court must have the appropriate security clearances.

V. Clerk's Office

Rule 7: Duties of the Clerk

(a) Duties: The Clerk will support the work of the Court consistent with the directives of the Presiding Judge. The Presiding Judge may permit the duties of the Clerk to be delegated.

(b) Court Records.
   (i) Maintenance of Court Records. The Clerk will: (A) maintain the Court's docket and records—including records and recordings of proceedings before the Court—and the seal; (B) accept all documents for filing; (C) keep all records, pleadings, and files in a secure location, making those materials available only to persons authorized to have access to them; and (D) perform any other duties, consistent with the usual powers of a Clerk of Court, as the Presiding Judge may authorize.
   (ii) Release of Court Records. Except when Orders or Opinions are provided to the government when issued, no Court records or other materials may be released without prior motion to and Order by the Court. Court records shall be released in conformance with the security measures referenced in Rule 3.

(c) Electronic Filing: The Clerk, when authorized by the Court, may accept and file applications, Orders, and other filings by any reliable, and appropriately secure, electronic means.

VI. Form and Filing of Applications for Court Orders

Rule 8: Form of Applications for Court Order

(a) Compliance With the Foreign Intelligence Surveillance Act: A Federal officer may file an application for a Court Order in accordance with the Foreign Intelligence Surveillance Act. The application must be approved and certified in accordance with the Act. The application must contain the statements and other information required by the Act.

(b) Citations: Each application must contain citations to pertinent provisions of the Act.
(c) Facsimile or Digital Signatures: With the Judge's consent, an application may be submitted by any reliable, and appropriately secure, electronic means, including facsimile.

**Rule 9: Time of Submission; Applications**

(a) Time of Submission: Other than for an application being submitted following the Attorney General's authorization of emergency physical search, electronic surveillance, or pen register/trap and trace surveillance, proposed applications and orders must be submitted at least seven calendar days before the date of the scheduled hearing. The final application with the Federal officer's written oath or affirmation, and the approval and certification required by the Act, may be submitted later, but no later than two hours before the scheduled hearing.

(b) Notice of Changes: The government may submit an amended application, but it must identify any differences from previous submissions at the time the Court reviews the final application.

**Rule 10: New Matters; Supplementation**

(a) Notice to the Court: If an application or other request for action involves an issue not previously before the Court—including, but not limited to, novel issues of technology or law—the applicant must inform the Judge of the nature and significance of that issue.

(i) Memorandum Relating to New Technology. Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court which: (A) explains the technique; (B) describes the circumstances of the likely use of the technique; (C) discusses legal issues apparently raised by the technique; and (D) describes proposed minimization procedures to be applied to the use of the technique. At the latest, the memorandum must be submitted as part of the first application that seeks to employ the new technique.

(ii) Legal Memorandum. If an application or other request for action raises an issue of law not previously considered by the Court, the government must submit a memorandum of law in support of its position on each new issue. At the latest, the memorandum must be submitted as part of the first application that raises the issue.

(b) Correction of Material Facts: If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of: (i) the misstatement or omission; (ii) any necessary correction; (iii) the facts and circumstances relevant to the misstatement or omission; (iv) any modifications the government has made or proposes to make in how it will implement any authority granted by the Court; and (v) how the government
proposes to dispose of or treat any information obtained as a result of the misstatement or omission.

(c) Disclosure of Non-Compliance: If the government discovers that any authority granted by the Court has been implemented in a manner that did not comply with the Court's authorization, the government, in writing, must immediately inform the Judge to whom the submission was made of: (i) the non-compliance; (ii) the facts and circumstances relevant to the non-compliance; (iii) any modifications the government has made or proposes to make in how it will implement any authority granted by the Court; and (iv) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

(d) Supplementation: The Court may require the applicant to furnish any information the reviewing Judge deems necessary for an informed review of that application and any proposed Orders relating to it.

Rule 11: Motions
Unless the Judge who issued the Order granting an application directs otherwise, a motion to amend the Order need not be presented to the Judge who issued it. The Judge to whom a motion is presented may refer the motion for review and determination to the Judge who ruled on the application.

Rule 12: Applications Following Approval of Emergency Authorizations
(a) Notification: A Judge who has been notified of the emergency authorization of electronic surveillance, physical search, or pen register/trap and trace surveillance pursuant to 50 U.S.C. § 1805(f), § 1824(e), or § 1843, may refer the consequent application to another Judge of the Court.

(b) Hearings: To the extent practicable, hearings on applications consequent to emergency authorizations shall be added to regularly scheduled court sessions.

VII. Hearings
Rule 13: Hearings
(a) Scheduling: The Judge to whom an application is presented shall set the time for the hearing.

(b) Ex Parte: Except as provided for under Rule 15, all hearings shall be ex parte and conducted in a secure location and manner.

(c) Appearances: Unless excused, the official supplying the factual information upon which an Order is sought and an attorney for the applicant must attend the
hearing, along with other representatives of the government as the Court may
direct or permit.

(d) Testimony; Oath; Recording of Proceedings: The Judge may take testimony
under oath and receive other evidence. The testimony may be recorded
electronically or as the Judge may otherwise direct, consistent with the security
measures referenced in Rule 3.

VIII. Orders

Rule 14: Contents
(a) Citations: All Orders must contain citations to pertinent provisions of the
Foreign Intelligence Surveillance Act.

(b) Denying Applications.
   (i) Written Statement of Reasons. If a Judge denies an application, the Judge
       must immediately prepare and file a written statement of each reason for the
decision and cause a copy of the statement to be served on the government.
   (ii) Submission of Previously Denied Applications. When a Judge denies an
application, further submission of the application may be made only to that
Judge.

(c) Approving Applications; Expiration Date: The expiration date and time of an
Order approving an application must be computed on the basis of calendar days,
not judicial business days, and must be stated as Eastern Time. Expiration dates
must be computed from the date and time of the Court's issuance of an Order, or,
if applicable, of the Attorney General's exercise of emergency authorization
pursuant to 50 U.S.C. § 1805(f), § 1824(e), or § 1843.

(d) Electronic Signatures: The Judge may sign the Order by any reliable, and
appropriately secure, electronic means, including facsimile.

Rule 15: Enforcement; Sanctions
(a) Show Cause Motions: If a person or entity served with a Court Order (the
"recipient") fails to comply with that Order, the government may move the Court
for an Order to show cause why the recipient should not be held in contempt and
sanctioned accordingly. The motion must be filed with the Clerk of the Court and
referred to the Judge of the Court who entered the underlying Order.

(b) Proceedings.
   (i) An Order to show cause must confirm issuance of the underlying Order,
schedule further proceedings, and afford the recipient an opportunity to show
cause why the recipient should not be held in contempt.
(ii) Proceedings on motions and Orders to show cause must be in camera. All records of such proceedings must be maintained in conformance with 50 U.S.C. § 1803(c).

(iii) If the recipient fails to show cause for noncompliance with the underlying Order, the Court may find the recipient in contempt and enter any further Orders it deems necessary and appropriate to compel compliance and to sanction the recipient for noncompliance with the underlying Order.

(iv) If the recipient shows cause for noncompliance or if the Court concludes that the underlying Order should not be enforced as issued, the Court may enter any further Orders it deems appropriate.

**Rule 16: Returns; Time for Filing; Contents**

(a) Time for Filing.

(i) Search Orders. Unless otherwise ordered by the Court, a return must be made following the issuance of a Search Order either at the time of submission of a renewal application or within ninety days of the execution of a Search Order, whichever is sooner.

(ii) Other Orders. The Court may order the filing of other returns at a time and in a manner as it deems appropriate.

(b) Contents: The return must: (i) notify the Court of the execution of the Order; (ii) describe the circumstances and results of the search or other activity including, where appropriate, an inventory; (iii) certify either that the execution was in conformity with the Order, or, if not in conformity, describe any deviation in execution from the Order and explain the reasons for any deviation; and (iv) include any other information as the Court may direct.

**IX. Sequestration or Destruction**

**Rule 17: Sequestration or Destruction**

If the government submits material for sequestration, the Presiding Judge may order the government to file a memorandum stating the circumstances of the material's acquisition, reasons for the request to sequester rather than destroy the material, and any other information as the Presiding Judge may direct. The Presiding Judge may direct the Clerk to keep the material, specifying the terms and conditions of its retention, or order the Clerk or the government to destroy the material.

**X. Appeals**

**Rule 18: Motion to Transmit Record**

The government may file an appeal within 60 days of the denial of an application. Upon filing the appeal, the government must file a motion to transmit the record
to the Foreign Intelligence Surveillance Court of Review (hereafter, "Court of Review").

Rule 19: Transmission of the Record
The Court must transmit the record under seal to the Court of Review as expeditiously as possible, and no later than 30 days after the government's motion. A copy of the Judge's statement of reasons denying the application must be included as part of the record on appeal.

Rule 20: Oral Notification to the Court of Review
The Clerk must orally notify the Presiding Judge of the Court of Review immediately upon receipt of a motion from the government to transmit a record to the Court of Review.
I: IN GENERAL

§ 1: Limited Scope
These procedures govern the filing and disposition of petitions pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, as amended (hereafter, "the Act").

§ 2: Rules of the Foreign Intelligence Surveillance Court Apply
These procedures supplement the Rules of Procedure of the Foreign Intelligence Surveillance Court (available at www.uscourts.gov/rules), which govern all matters before this Court.

Table of Contents

- I: IN GENERAL
- II: PETITION AND OTHER PAPERS
- III: ASSIGNMENT TO A JUDGE
- IV: CONSIDERATION OF PETITION
II: PETITION AND OTHER PAPERS

§ 3: Filing
(a) Who May File: The recipient of an Order to produce a tangible thing under Section 501 of the Act may file a petition challenging the Order pursuant to Section 501(f) of the Act. A petition may be filed through counsel.

(i) Petitioner's Initial Filing. The petition or other paper initially filed shall include the petitioner's full name, mailing address, email address, and telephone number. If the petitioner is represented by counsel, the petition or other paper initially filed shall include the petitioner's full name and the full name of the petitioner's attorney, as well as the attorney's address, telephone number, email address, facsimile number, and bar membership information.

(ii) Government's Initial Filing. The government's initial response shall include the full name of the attorneys representing the United States, and their mailing addresses, email addresses, telephone numbers, and facsimile numbers.

(b) Where to File.

(i) Challenging an Unclassified Order. Filing a petition and any related papers challenging an unclassified Production Order or Nondisclosure Order may be accomplished by hand delivery or by overnight delivery to the Foreign Intelligence Surveillance Court’s Security Officer (hereafter, "the Court Security Officer"), c/o Security and Emergency Planning Staff, United States Department of Justice, Room 6217, 950 Pennsylvania Ave., NW, Washington, DC 20530. A signed original and one copy of all papers must be submitted.

(ii) Challenging a Classified Order. Filing a petition and any related papers challenging a classified Production Order or Nondisclosure Order (i.e., marked Confidential, Secret, or Top Secret), may be accomplished by contacting the Court Security Officer by telephone to receive instructions about how to file and serve the petition and any related papers. (The Court Security Officer may be contacted by calling the Department of Justice Command Center at 202-514-5000, and asking to be directed to the Director, Security and Emergency Planning Staff).

(c) Time to File Petition.

(i) Challenging a Production Order. A petition challenging an Order to produce a tangible thing must be filed within 20 days after the Order has been served.

(ii) Challenging a Nondisclosure Order. A petition challenging a Nondisclosure Order issued under Section 501(d) may not be filed with this Court earlier than one year after the date of the issuance of the Production Order containing the challenged Nondisclosure Order.

(iii) Subsequent Petition Challenging a Nondisclosure Order. If a Judge denies a petition to modify or set aside a Nondisclosure Order, the petitioner may not file with this Court a subsequent petition challenging the same Nondisclosure Order earlier than one year after the date of the denial.

(d) Effective Date of Filing.
(i) By Petitioner. A petition or other papers submitted by the petitioner shall be considered to be filed on the date received by the Court Security Officer. The Court Security Officer shall transmit all submissions to the Clerk of the Foreign Intelligence Surveillance Court (hereafter, "the Clerk of the Court") on the same date that they are received.

(ii) By Government. The government's response and other papers submitted by the government shall be considered to be filed on the date that they are received by the Clerk of the Court.

§ 4: Content of Petition
(a) Grounds for Petition: A petition shall concisely state the factual and legal grounds for modifying or setting aside the challenged Order.

(b) Access to Classified Information: A petition shall state whether the petitioner and/or the petitioner's attorney previously have been provided access to classified information and the circumstances of such access.

(c) Request to Stay Production.
   (i) Petition Does Not Automatically Effect a Stay. A petition does not automatically effect a stay of the underlying Order. In order to stay a Production Order, petitioner must request such relief and it must be granted by the judge to whom the matter is assigned.
   (ii) Stay May Be Requested Prior to Filing of a Petition. A petitioner may request a stay of a Production Order prior to filing a petition challenging such Order.

(d) Underlying Order: A petition shall include a copy of the Production Order to which it relates and state the date on which such Order was served upon petitioner.

(e) Petitioner's Request for Hearing: A petition shall state whether a hearing is requested and, if so, whether the petitioner (or petitioner's counsel) seeks to appear personally in the Washington, D.C., area at petitioner's expense, or to participate in a hearing via teleconference.

§ 5: Form and Length of Petition and Other Papers
(a) Form: A petition and other papers filed shall be:
   (i) on 8 1/2 by 11 inch opaque white paper;
   (ii) typed (double space) or reproduced in a manner that produces a clear black image;
   (iii) conspicuously marked "SECTION 501(f) PETITION" on the document itself and any accompanying envelope; and
   (iv) filed under seal.

(b) Length.
(i) Petition. Unless otherwise authorized by the assigned Judge, a petition shall not exceed 20 pages in length, including any attachment.

(ii) Other Papers.

(A) Government's Response. Unless otherwise authorized by the assigned Judge, the government's response shall not exceed 20 pages in length, including any attachment.

(B) Petitioner's Reply. Unless otherwise authorized by the assigned Judge, the petitioner's reply, if any, shall not exceed 10 pages in length, including any attachment.

(C) Additional Papers. No sur-replies may be filed without leave of the Court.

§ 6: Service

(a) By Petitioner: A petitioner shall, at or before the time of filing a petition or other paper, serve a copy by hand delivery or by overnight delivery on the United States Department of Justice, National Security Division, 950 Pennsylvania Ave., NW, Room 6150, Washington, D.C. 20530 and on the Federal Bureau of Investigation, Office of General Counsel, National Security Law Branch, 935 Pennsylvania Ave., NW, Room 7947, Washington, D.C. 20535.

(b) By Government: The government shall, at or before the time of filing a response or other paper, serve a copy by hand delivery or by overnight delivery on petitioner's counsel of record or, if the petitioner is proceeding pro se, on the petitioner.

§ 7: Computation of Time

In proceedings governed by these procedures, any period of time shall be computed in the manner specified in Rule 6(a) of the Federal Rules of Civil Procedure. The provisions of Rule 6(e) of the Federal Rules of Civil Procedure shall not apply to the computation of time in these proceedings.

§ 8: Notifying Presiding Judge

Upon receipt, the Clerk of the Court shall notify the Presiding Judge of the Foreign Intelligence Surveillance Court that a petition has been received from the Court Security Officer.

(a) Presiding Judge Unavailable: If the Presiding Judge is not reasonably available when the Clerk of the Court receives a petition, the Clerk of the Court shall notify the local Judge, other than the Presiding Judge, who has the most seniority on the Court. If no local Judge is reasonably available, the Clerk of the Court shall notify the Judge with the most seniority on the Foreign Intelligence Surveillance Court who is reasonably available. The Judge who receives notification shall be the Acting Presiding Judge (hereafter, "the Presiding Judge") for the case.
III: ASSIGNMENT TO A JUDGE

§ 9: Assignment
(a) Presiding Judge: Immediately upon receiving notification from the Clerk of the Court that a petition has been filed, the Presiding Judge shall assign the matter to a Foreign Intelligence Surveillance Court Judge in the petition review pool (hereafter, "the Judge"). The Clerk of the Court shall record the date and time of the assignment.

(b) Transmitting Petition: As soon as possible, and no later than 24 hours after being notified by the Presiding Judge that a petition has been assigned to one of the pool Judges, the Clerk of the Court shall transmit the original or a copy of petition to that Judge.

IV: CONSIDERATION OF PETITION

§ 10: Initial Review
(a) When: The Judge shall conduct an initial review of the petition within 72 hours after being assigned the petition.

(b) Frivolous Petition: If the Judge determines that the petition is frivolous, the Judge shall:
   (i) immediately deny the petition and affirm the challenged Order;
   (ii) promptly provide a written statement of the reasons for the denial; and
   (iii) provide a written ruling, together with the statement of reasons, to the Clerk of the Court, who will transmit them to the Court Security Officer for immediate delivery to the petitioner and the government.

(c) Non-Frivolous Petition.
   (i) Scheduling. If the Judge determines that the petition is not frivolous, the Judge shall promptly issue an Order that sets a schedule for its consideration. The Clerk of the Court shall transmit a copy of the Order to the petitioner and the government.
   (ii) Manner of Proceeding. At the Judge's discretion, a hearing may be held or the proceedings may be conducted solely on the papers submitted by the petitioner and the government.

§ 11: Response and Reply
(a) Government's Response: Unless otherwise ordered by the Judge, the government's response must be filed within 20 days after the issuance of the initial scheduling order. If the government's response, or any other paper the government is permitted to file, contains classified information that is submitted ex parte, the government also shall file with the Court and serve on the petitioner an unclassified or redacted version. The unclassified or redacted version, at a minimum, should clearly articulate the government's legal arguments.
(b) Petitioner's Reply: The petitioner may file a reply to the government's response within 10 days after the date the government's response is served.

§ 12: Hearing
(a) Request: The petitioner or the government may request a hearing.

(b) Location: Hearings shall be held in the Washington D.C. area at a location to be determined by the Judge.

(c) In Camera: All hearings shall be in camera.

(d) Recording: All hearings shall be recorded, either by sound or stenographic means.

§ 13: Ex Parte Proceedings
At the request of the government, the Judge shall review ex parte and in camera any papers submitted by the government, or portions thereof, which may include classified information.

§ 14: Rulings on Non-frivolous Petitions
(a) Written Statement of Reasons: The Judge shall promptly provide a written statement of the reasons for modifying, setting aside, or affirming a Production or Nondisclosure Order. The statement may include classified information.

(b) Reinstatement of Underlying Order: If the Judge does not modify or set aside the underlying Order, the Judge shall immediately affirm it and order the recipient to comply therewith.

(c) Transmitting the Judge's Ruling: The Clerk of the Court shall transmit the Judge's ruling and written statement of reasons to the Court Security Officer for immediate delivery to the petitioner and the government. If the Judge's ruling or written statement contains classified information, an unclassified or redacted version shall be provided to the petitioner.

§ 15: Appeals and Sanctions
(a) Appeals: The government or the petitioner may request the Foreign Intelligence Surveillance Court of Review to review the Judge's ruling.

(b) Failure to Comply: If a recipient fails to comply with an Order affirmed under Section 501(f) of the Act and these procedures, the government, pursuant to Rule 15 of the Foreign Intelligence Surveillance Court Rules of Procedure, may file a motion with the Foreign Intelligence Surveillance Court (for referral to the Judge
of the Court who entered the underlying Order) seeking enforcement of the affirmed Order. The Court may consider the government's motion without convening further proceedings on the matter.
Rule 1: Name of Court
This Court, established pursuant to the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, Title IV, 110 Stat. 1214, 1258, (Title V of the Immigration and Nationality Act), and as amended by the Omnibus Consolidated Appropriations Act for 1997, Public Law No. 104-208, Title I, § 354, 110 Stat. 3009, shall be known as the Alien Terrorist Removal Court of the United States (8 U.S.C. § 1531 et seq.).

Rule 2: Seal
The seal of the Court shall contain the words "Alien Terrorist Removal Court" in the upper sector of space included within the two outer concentric circles and the words "of the United States of America" in the lower sector, and shall contain the standardized eagle rampant in the center.

Rule 3: Situs
The situs of the Court shall be at the United States Courthouse, Washington, D.C., 20001.

Rule 4: Clerk
(a) The Clerk of the District Court for the District of Columbia shall be the Clerk of this Court.

(b) The Clerk shall supply a deputy clerk and other personnel as the business of this Court may require.

(c) Personnel responsible for filing and maintaining records of this Court containing classified information shall have appropriate levels of security clearance in compliance with Executive Branch procedures governing classified information.
Rule 5: Application for Removal
(a) The Attorney General, acting on behalf of the United States as applicant, shall file an original and two copies of an application seeking removal of an alleged alien, named as respondent.

(b) The application shall be submitted ex parte and in camera and shall be filed under seal with the Clerk of this Court.

(c) The application shall state, to the extent known, the level of classified information, if any, that the Attorney General will present in support of removal.

(d) The application shall state whether the respondent is a permanent resident alien.

Rule 6: Assignment of Cases
(a) The Clerk shall promptly advise the Chief Judge, by a secured means, of the filing of an application. The Chief Judge shall thereupon make an assignment of the case to a member of the Court for consideration and determination of that case.

(b) Cases shall be assigned to judges of the Court in such a manner that each judge, if available for an assignment, shall receive an assignment before any other judge receives a second or successive assignment.

Rule 7: Service of an Order Granting an Application and Notice of a Removal Hearing
(a) If an order is entered granting an ex parte application, an authorized representative of the Attorney General shall serve the respondent who is the subject of the application with a copy of the order, excluding any classified information in the order, together with a Notice pursuant to 8 U.S.C. § 1534(b). The Notice shall also set an expeditious date for the Removal Hearing.

(b) The Attorney General shall file with the Clerk a certificate of service of the order and Notice.

(c) Retained counsel for a respondent shall promptly file an appearance with the Clerk.

(d) If a respondent is financially unable to obtain adequate representation, the respondent may request appointment of counsel from the Criminal Justice Panel for United States District Court for the District of Columbia, as provided for in Section 3006A of Title 18 (Criminal Justice Act).
Rule 8: Interim Hearing
(a) For the convenience of the assigned judge and the parties, the judge may conduct an Interim Hearing or Hearings for the purpose of resolving issues relating to representation of the respondent, special issues relating to a permanent resident alien respondent, issues relating to classified information, or if required by statute. When appropriate, the Interim Hearing will be conducted ex parte and in camera.

(b) Any Interim Hearing shall be conducted in the United States Courthouse in Washington, D.C.

Rule 9: Place of Conducting Removal Hearing
The Removal Hearing shall be held in the United States Courthouse in Washington, D.C. The Removal Hearing shall be conducted publicly, except that any part of the argument that refers to evidence received in camera and ex parte, shall be heard in camera and ex parte.

Rule 10: Verbatim Record of Proceedings
All ex parte, in camera, and public hearings of the Court shall be recorded verbatim by a reporter retained pursuant to 28 U.S.C. § 753, by shorthand, mechanical means, electronic sound recording, or any other method, subject to regulations promulgated by the Judicial Conference of the United States.

Rule 11: Motions
(a) Any motion shall include or be accompanied by a statement of the specific points of law and authority that support the motion, including where appropriate a concise statement of facts. If a table of cases is provided, counsel shall place asterisks in the margin to the left of those cases or authorities on which counsel chiefly relies.

(b) Within 15 days of the date of service or at such other time as the assigned judge may direct, an opposing party shall serve and file a memorandum of points and authorities in opposition to the motion. If such a memorandum is not filed within the prescribed time, the judge may treat the motion as uncontested.

(c) Each motion shall be accompanied by a proposed order.

(d) Within 10 days after service of the memorandum in opposition, the moving party may serve and file a reply memorandum.
(e) A memorandum of points and authorities in support of or in opposition to a motion shall not exceed 15 pages and a reply memorandum shall not exceed 10 pages, without prior approval of the assigned judge.

(f) A party may in a motion or opposition request oral argument, but its allowance shall be within the discretion of the assigned judge.

**Rule 12: Subpoenas**
Except for good cause shown, requests for issuance of a subpoena pursuant to 8 U.S.C. § 1534(d) by either the respondent or applicant, shall be made at least 10 days prior to the date of the removal hearing.

**Rule 13: Classified Information**
(a) The ex parte and in camera examination of any classified information, pursuant to 8 U.S.C. § 1534(e)(3)(A)-(E), and of the proposed unclassified summary of specific information shall both be conducted on the day of the Interim Hearing unless the assigned judge otherwise directs.

(b) The unclassified summary, following approval by the judge, shall be delivered to the respondent without delay.

(c) When the respondent is a lawful permanent resident alien, who is denied an unclassified summary pursuant to 8 U.S.C. § 1534(e)(3)(F), the judge shall designate a special attorney to assist the respondent by reviewing the classified information.

(d) When the appointed special attorney moves to challenge the veracity of the evidence contained in the classified information pursuant to 8 U.S.C. § 1534(e)(3)(F)(i)(II), the assigned judge shall schedule an in camera proceeding prior to the Removal Hearing to consider the motion.

**Rule 14: Removal Hearing Memorandum**
Seven days prior to the Removal Hearing, counsel for the applicant and the respondent shall file with the Clerk and serve on each other a Hearing Memorandum setting forth any legal issues to be raised, a summary of the anticipated testimony (exclusive of classified information), and copies of exhibits (exclusive of classified information). The names of individuals involved in the investigation and prospective witnesses need not be included in the material filed with the Court.