SECURITY PROGRAM OPERATING MANUAL

DATE 12/21/2010

Version 3.0

U.S. Department of Justice

Justice Management Division

Security and Emergency Planning Staff

Washington, D.C. 20530

DEC 21 2010

FOREWORD

As the Department Security Officer, I am pleased to promulgate the revised Department of Justice Security Program Operating Manual (SPOM) for the protection of classified National Security Information (NSI) and Sensitive but Unclassified (SBU) information. The manual was revised in coordination with Department components, and it reflects the efforts of many individuals and organizations. I want to thank all of you for your assistance.

The SPOM establishes uniform security policies and operational procedures within the Department for the protection of NSI and SBU information consistent with national safeguarding standards for such information, including those derived from Executive Order 13526, Classified National Security Information. It provides a comprehensive source of information to facilitate the proper implementation of the policies and procedures established for the protection of information and technologies vital to our national security.

The Security and Emergency Planning Staff (SEPS) will continue to work with Department components to revise the SPOM as necessary and incorporate additional guidance when promulgated by Executive Agents. Users of the SPOM are encouraged to send comments and suggestions through their Security Programs Manager to the SEPS, Robert F. Kennedy Main Justice Building, 950 Pennsylvania Avenue, Room 6217, Washington, DC 20530.

James L. Dunlap
Department Security Officer

Table of Contents

SECURITY PROGRAM OPERATING MANUAL **1**

FORWARD **2**

TABLE OF CONTENTS **3**

CHAPTER 1 GENERAL PROVISIONS AND REQUIREMENTS **5**

SECTION 1. INTRODUCTION 5
SECTION 2. GENERAL REQUIREMENTS 5
SECTION 3. REPORTING REQUIREMENTS 6

CHAPTER 2 ACCESS TO CLASSIFIED INFORMATION **9**

SECTION 1. REQUIREMENTS FOR ACCESS 9
SECTION 2. FINANCIAL INFORMATION REQUIRED 10
SECTION 3. OBTAINING ACCESS AUTHORIZATIONS 11
SECTION 4. ACCESS BY PERSONS OUTSIDE THE EXECUTIVE BRANCH 12
SECTION 5. DENIAL OR REVOCATION OF ACCESS 13

CHAPTER 3 SECURITY EDUCATION **15**

SECTION 1. SECURITY EDUCATION AND TRAINING 15
SECTION 2. INITIAL TRAINING 15
SECTION 3. ANNUAL REFRESHER TRAINING AND TERMINATION BRIEFINGS 16
SECTION 4. OTHER TRAINING REQUIREMENTS 17

CHAPTER 4 CLASSIFICATION MANAGEMENT **18**

SECTION 1. ORIGINAL CLASSIFICATION 18
SECTION 2. DERIVATIVE CLASSIFICATION 23
SECTION 3. DECLASSIFICATION AND DOWNGRADING 24

CHAPTER 5 MARKING CLASSIFIED INFORMATION **32**

SECTION 1. INTRODUCTION 32
SECTION 2. ORIGINAL CLASSIFICATION MARKINGS 32
SECTION 3. DERIVATIVE CLASSIFICATION MARKINGS 34
SECTION 4. MARKING IN THE ELECTRONIC ENVIRONMENT. 35
SECTION 5. ADDITIONAL REQUIREMENTS 38
SECTION 6. DECLASSIFICATION MARKINGS 40
SECTION 7. SPECIAL REQUIREMENTS FOR RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATA (FRD) DOCUMENTS 41
SECTION 8. CONTROLLED UNCLASSIFIED INFORMATION. 43

CHAPTER 6 SAFEGUARDING REQUIREMENTS **44**

SECTION 1. GENERAL REQUIREMENTS 44
SECTION 2. STANDARDS FOR SECURITY EQUIPMENT 44
SECTION 3. STORAGE OF CLASSIFIED INFORMATION 44
SECTION 4. INFORMATION CONTROLS 45
SECTION 5. TRANSMISSION 46
SECTION 6. DESTRUCTION 48
SECTION 7. LOSS, POSSIBLE COMPROMISE OR UNAUTHORIZED DISCLOSURE. 49
SECTION 8. OPEN STORAGE AREAS 49
SECTION 9. OFFICE PROCEDURES FOR SAFEGUARDING CLASSIFIED INFORMATION. 50
SECTION 10. EMERGENCY AUTHORIZATION FOR DISCLOSURE. 51
SECTION 11. PERFORMANCE RATINGS 51

CHAPTER 7 FOREIGN GOVERNMENT INFORMATION **52**

SECTION 1. GENERAL 52
SECTION 2. SAFEGUARDING REQUIREMENTS 52
SECTION 3. FOREIGN DISCLOSURE OF CLASSIFIED U.S. GOVERNMENT INFORMATION. 54

CHAPTER 8 INFORMATION ASSURANCE **55**

SECTION 1. POLICY AND RESPONSIBILITIES 55
SECTION 2. MINIMUM SECURITY REQUIREMENTS 56
SECTION 3. ADDITIONAL PROVISIONS 59

CHAPTER 9 COMMUNICATIONS SECURITY **62**

CHAPTER 10 RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS **64**

SECTION 1. CLASSIFIED CONTRACTS 64
SECTION 2. CLASSIFIED CONTRACTOR VISITS 65

CHAPTER 11 SPECIAL ACCESS PROGRAMS **67**

SECTION 1. INTRODUCTION 67
SECTION 2. ADMINISTRATION OF THE SCI PROGRAM 68
SECTION 3. SCI ACCESS AUTHORIZATIONS 68
SECTION 4. SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF) 69
SECTION 5. SCI COMPUTER SYSTEMS 70
SECTION 6. CLEARANCE CERTIFICATIONS 70

CHAPTER 12 ACCOUNTING FOR COST **72**

SECTION 1. INTRODUCTION 72
SECTION 2. COST CATEGORIES 72

CHAPTER 13 SELF-INSPECTION REVIEW PROGRAM **75**

SECTION 1. INTRODUCTION 75
SECTION 2. ELEMENTS OF REVIEW 76

CHAPTER 14 RESTRICTED DATA AND FORMERLY RESTRICTED DATA **78**

SECTION 1. INTRODUCTION 78
SECTION 2. QUALIFICATIONS AND DESIGNATIONS 79
SECTION 3. TRAINING REQUIREMENTS 79
SECTION 4. CLASSIFICATION GUIDANCE 79
SECTION 5. CLASSIFYING RD AND FRD DOCUMENTS 80
SECTION 6. DECLASSIFYING RD AND FRD DOCUMENTS 80
SECTION 7. ADMINISTRATIVE POLICIES AND PROCEDURES 80

CHAPTER 15 REPORTING OF SECURITY CLASSIFICATION MANAGEMENT PROGRAM DATA **82**

SECTION 1. INTRODUCTION 82
SECTION 2. CLASSIFICATION PROGRAM MANAGEMENT CATEGORIES. 82

CHAPTER 16 CONTROLLED UNCLASSIFIED INFORMATION **86**

RESERVED 86

ANNEX A GLOSSARY OF SECURITY TERMS **87**

ANNEX B ACRONYM LIST **92**

ANNEX C ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION AND TO SENSITIVE COMPARTMENTED INFORMATION AND SPECIAL ACCESS PROGRAMS **94**

SECTION 1. INTRODUCTION 94
SECTION 2. THE ADJUDICATIVE PROCESS 94

ANNEX D INVESTIGATIVE STANDARDS FOR BACKGROUND INVESTIGATIONS FOR ACCESS TO CLASSIFIED INFORMATION **96**

SECTION 1. INTRODUCTION 96
SECTION 2. GENERAL INFORMATION 96
SECTION 3. STANDARD FOR ACCESS TO CONFIDENTIAL AND SECRET INFORMATION 96
SECTION 4. STANDARD FOR ACCESS TO TOP SECRET AND SENSITIVE COMPARTMENTED INFORMATION (SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)) 97
SECTION 5. STANDARD FOR PERIODIC REINVESTIGATIONS. (PHASED PERIODIC REINVESTIGATION (PPR) OR SINGLE SCOPE BACKGROUND INVESTIGATION--PERIODIC REINVESTIGATION (SSBI-PR)). 97
SECTION 6. INVESTIGATIVE STANDARDS FOR TEMPORARY ELIGIBILITY FOR ACCESS. 97

ANNEX E GUIDELINES FOR CONSTRUCTION OF OPEN STORAGE AREAS **99**

SECTION 1. INTRODUCTION 99
SECTION 2. GENERAL. 99
SECTION 3. CONSTRUCTION REQUIREMENTS FOR OPEN STORAGE AREAS. 99

ANNEX F INTRUSION DETECTION SYSTEM STANDARDS **101**

SECTION 1. GENERAL 101
SECTION 2. DSO APPROVAL 101
SECTION 3. CENTRAL MONITORING STATION 101
SECTION 4. INVESTIGATIVE RESPONSE TO ALARMS. 101
SECTION 5. INSTALLATION. 102
SECTION 6. CERTIFICATION OF COMPLIANCE. 102
SECTION 7. EXCEPTIONAL CASES 102

ANNEX G SANITIZING AND RELEASING COMPUTER COMPONENTS **103**

SECTION 1. GENERAL 103
SECTION 2. GENERAL REQUIREMENTS. 103
SECTION 3. SPECIFIC DEVICE PROCEDURES 104
SECTION 4. SECURITY INSPECTION AND RELEASE FORM 107

ANNEX H SAFEGUARDING CLASSIFIED INFORMATION ON LAPTOP/NOTEBOOK COMPUTERS **109**

SECTION 1. INTRODUCTION 109
SECTION 2. TRANSPORTING LAPTOPS IN AND OUT OF A SCIF. 109
SECTION 3. TRAVELING WITH CLASSIFIED LAPTOPS 109

ANNEX I REPRODUCTION ON DIGITAL EQUIPMENT **110**

SECTION 1. INTRODUCTION 110
SECTION 2. DIGITAL COPIERS 110
SECTION 3. POLICY 110
SECTION 4. PROCEDURES FOR CLASSIFIED DIGITAL COPIERS 110
SECTION 5. PROCEDURES FOR UNCLASSIFIED DIGITAL COPIERS 111

ANNEX J REFERENCES **112**

Chapter 1
General Provisions and Requirements

Section 1.
Introduction

1-100. Purpose. This manual prescribes requirements and procedures for the classification, safeguarding and declassification of Classified National Security Information (NSI) and specified portions of the control and protection of Sensitive But Unclassified Information within the Department of Justice (DOJ). The manual also prescribes requirements and safeguards necessary for Sensitive Compartmented Information (SCI) and other Special Access Programs (SAPs). Finally, the manual prescribes a monitoring system to enhance its effectiveness. This manual supersedes all previous versions of the manual.

1-101. Authority. Executive Orders (EO) 13526, "Classified National Security Information," 12968, as amended, "Access to Classified Information," 12829, as amended, "National Industrial Security Program," 12333, as amended, "United States Intelligence Activities," 32 CFR Part 2001, "the Directive," and 28 CFR Part 17, "Classified National Security Information and Access to Classified Information."

1-102. Scope. The provisions of this manual apply to all DOJ personnel including employees, contractors, detailees and other persons granted a security clearance or access to DOJ facilities and information through the Security and Emergency Planning Staff's (SEPS) Litigation Security Group (LSG) and/or access under a U.S. Court Protective Order, unless otherwise indicated. DOJ employees performing work at other U.S. Government agency facilities shall safeguard classified information in accordance with the provisions of this manual and/or in accordance with the procedures established by the host facility. If a DOJ employee believes he or she cannot comply with both sets of requirements, the employee should consult with the Security Programs Manager (SPM) of his or her component.

1-103. Definitions. A glossary of terms is contained in Annex A.

1-104. Acronyms. All acronyms used in this document are listed and defined in Annex B.

1-105. Forms. Hyperlinks are provided in the text of this manual for the various forms mentioned within.

1-106. Suggested Improvements. Users are invited to send comments and suggestions through the SPM to the DOJ SEPS, Robert F. Kennedy Main Justice Building, 950 Pennsylvania Avenue, Room 6217, Washington, DC 20530-0001.

1-107. Publication in the *Federal Register*. Regulations contained in this manual shall be published in the *Federal Register* to the extent that they affect members of the public.

Section 2.
General Requirements

1-200. Responsibilities.

a. Senior Agency Official. The Attorney General has designated the Assistant Attorney General for Administration as the Senior Agency Official (SAO) responsible to direct and administer the DOJ's classified information security program in accordance with EO 13526.

b. Department Security Officer. The SAO has further designated the Department Security Officer (DSO) to direct, administer, and oversee the following functions of the DOJ's classified information security program. The DSO shall be responsible for:

(1) Develop and promulgate policy, procedures, and programs necessary for the implementation of the DOJ's classified information security program.

(2) Monitor, evaluate, and report the administration of DOJ's classified information security program.

(3) Ensure components establish and maintain an ongoing self-inspection program, to include periodic reviews and assessments of their classified and sensitive products.

(4) Establish a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the DOJ and to provide guidance to personnel on proper classification.

c. Chief Information Officer. See Chapter 8, Section 8-104 of this manual.

d. Heads of Components. The head of each component shall appoint and oversee a SPM who shall implement the provisions of this manual applicable to their component. Heads of Components must report the appointment of an SPM to the DSO.

e. Security Programs Managers. Component SPMs are responsible for implementing the provisions of this manual applicable to their component. SPM responsibilities are also included in DOJ Order 2600.2C, Security Programs and Responsibilities, or its successor. SPMs must receive training from the DSO regarding their responsibilities within 6 months of their appointment.

f. Security Representatives. Security Representatives implement the classified national security program for offices within the Justice Management Division. Additionally, Component SPMs may appoint and oversee

Security Representatives in assisting them with implementing the program within their component. SPMs must report all appointments of Security Representatives to the DSO. Security Representatives must receive training from the DSO regarding their responsibilities within 6 months of their appointment.

g. DOJ Personnel. All DOJ personnel, as referenced in Paragraph 1-102, regardless of grade, title, or position, have responsibility to safeguard information, related to national security, to which they have access. All DOJ personnel will report, to the proper authority, the violations by themselves and others that could lead to the unauthorized disclosure of classified and sensitive information. In addition, all DOJ personnel will immediately self report, in writing, any arrest and any on or off-duty allegations of misconduct to their supervisor or a higher level official in the chain of command and to the relevant component SPM. This responsibility cannot be waived, delegated, or in any other respect, excused. All DOJ personnel will safeguard all information and material, related to national security, especially classified information, which they access, and will follow the requirements of this and other applicable directives.

1-201. Sanctions. DOJ personnel will be subject to sanctions if they knowingly, willfully, or negligently disclose classified or sensitive information to unauthorized personnel. Sanctions can include, but are not limited to a warning, reprimand, suspension without pay, forfeiture of pay, removal, and loss or denial of access to classified information. Action can also be taken under applicable criminal law, if warranted.

1-202. Supplementation. Each component shall implement the applicable provisions of this manual. Additional written procedures shall be prepared only when the component believes them necessary for the effective implementation of this manual or when the DSO determines them necessary to reasonably preclude the possibility of loss or compromise of classified information. Components choosing to prepare additional written procedures must submit them to the DSO for review and approval prior to implementation.

1-203. Interpretations of Manual. Requests for interpretation of this manual should be made through the SPM to the DSO.

1-204. Waivers to the Manual. Requests for waivers of requirements in this manual shall be submitted in writing through the SPM to the DSO. Waiver requests must specify why it is impractical or unreasonable to comply with the requirement.

1-205. Security Updates. The DSO will periodically publish and distribute updates to the components providing notification of proposed or approved changes to or interpretations of the manual on the SEPS webpage at http://dojnet.doj.gov/jmd/seps/spom.html.

1-206. Security Reviews.

a. Representatives of the DSO shall conduct periodic reviews of components to ensure the safeguards employed are consistent with those outlined in this manual and are adequate for the protection of classified information. Components normally will be provided advance notice of the review. Unannounced reviews may be conducted at the discretion of the DSO.

b. SPMs shall conduct annual self inspections as detailed in Chapter 13 of this manual.

Section 3.
Reporting Requirements

1-300. General. Components shall report to the DSO any information pertaining to an employee's eligibility for access to classified information, the proper safeguarding of classified information, or the possible loss or compromise of classified information. Components shall ensure cleared employees are aware of their responsibility for reporting such information.

1-301. Reports to Servicing Personnel Security Office. Components shall submit the following reports to the appropriate personnel security office through the SPM regarding employees authorized for access to, or being considered for authorized access to, classified information:

a. Adverse Information. The component SPM shall report any adverse information concerning an employee authorized for access to classified information, or who is being considered for such access. This report shall be submitted even if employment of the individual has been terminated. To the extent practical, the report should contain: the subject's last, first, and middle name; social security number; date and place of birth; clearance level and date of clearance; employment status (if terminated, include termination date); the adverse information being reported; and the name and telephone number of the person who provided the adverse information if not self reported. For purposes of this paragraph, "adverse information" means particular information (not rumor or innuendo) tending to reflect unfavorably on whether the subject of the report(s) having access to classified information is clearly consistent with the interests of national security, based on the factors discussed in Annex C.

b. Change in Cleared Employee Status. Reports of an employee's death; change of name; change in position sensitivity; termination of employment; layoff or leave of absence for an indefinite period or a period exceeding one year; or residence or assignment outside the U.S., Puerto Rico, Guam or the Virgin Islands for a period exceeding 90 consecutive days.

c. Foreign Interest Representative. Reports that an employee has become or has ceased to be a Representative of a Foreign Interest (RFI).

d. Employees Desiring Not to Perform on Classified Work. Reports that an employee no longer wishes to be considered for access to classified information or no longer

desires to continue his or her existing authorization for access.

e. Standard Form 312. Reports that an employee has refused to execute the Classified Information Nondisclosure Agreement (Standard Form 312) and/or a debriefing statement.

1-302. Incident and Vulnerability Reporting. The following reports shall be submitted to the DSO through the SPM:

a. Reports of Possible Loss, Compromise or Suspected Compromise. Any incident involving a possible loss, compromise, or suspected compromise of sensitive or classified information, foreign or domestic, shall be reported to the DSO through the SPM and to the Justice Security Operations Center (JSOC) via email (dojcert@usdoj.gov), phone ((202) 305-5332), or the JSOC Remedy Portal in coordination with the Component IT Security Manager.

b. Suspicious Contacts. Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise an employee authorized access must be reported. In addition, all employee contacts with known or suspected intelligence officers of any foreign country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country, shall be reported.

c. Inability to Safeguard Classified Material. Any emergency situation that renders a facility incapable of safeguarding classified material shall be reported.

d. Security Equipment Vulnerabilities. Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and information technology system (IT) security hardware and software used to protect classified information. Reports of security equipment vulnerabilities containing classified information must be made through appropriate secure means. For classification guidance regarding security equipment vulnerabilities, see the Department of Justice Classification Guide, dated February 19, 2009, or its successor. For guidance regarding COMSEC violation refer to the DOJ COMSEC Manual.

e. Unauthorized Receipt of Classified Material. The receipt or discovery of any classified material that an employee is not authorized to have. The report should identify the source of the material, originator, quantity, an unclassified subject or title, date, and classification level.

f. Delays. A delay of more than 48 hours in the delivery of classified material by a commercial carrier shall be reported.

g. Information Technology Incidents. Any event involving IT systems, equipment or media which may result in disclosure of classified information to unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of computer system media, shall be reported.

h. Evidence of Tampering. Any evidence of tampering with a shipment, delivery, or mailing containing classified information shall be reported.

i. Unauthorized Transmission Methods. Any shipment or transmission of classified information that is received by other than an approved method prescribed by this manual shall be reported.

j. Purposeful Violations. Any incidents that indicate an employee knowingly or willfully violated security policies established for the protection of classified or sensitive information shall be reported.

k. Continued Eligibility for Access. Any information that raises doubt as to whether an employee's continued eligibility for access to classified information is clearly consistent with the national security shall be reported.

l. Reports of Loss and/or Theft of Federally Controlled Property. Any incident involving the loss and/or theft of federally controlled property including, but not limited to items such as firearms and laptop computers, shall be reported

1-303. Reporting Procedures.

a. Immediately after receiving a security incident report, under Paragraph 1-302, the SPM shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the incident. To the extent that an incident involves personally identifiable information, the SPM should ensure that the DOJ's Incident Response Procedures for Data Breaches Involving Personally Identifiable Information are also followed. The following information shall be determined during the preliminary inquiry and included in the initial report:

(1) What is alleged to have happened, and where and when the incident took place;

(2) Who reported the incident, to whom, and when;

(3) What classified information is involved; (Attach an unclassified listing of the classified material.)

(4) What is the classification level of the information involved;

(5) Who are the originators of the information;

(6) When, for how long, and under what circumstances was classified information vulnerable to unauthorized disclosure. Determine the identity of unauthorized

persons likely to have had access to the information; and

(7) What actions were taken (e.g., inventories, securing of material, changing of combinations, etc.) to secure the classified information and/or limit the damage before the inquiry began.

b. If the preliminary inquiry confirms: (i) that a loss, compromise, or suspected compromise of classified information occurred, or (ii) that a security violation involving classified information occurred, the SPM shall immediately submit an initial report. Submission of the initial report must not be deferred pending completion of the entire investigation.

(1) Initial reports of suspected violations involving 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, shall be submitted to the DOJ Office of Professional Responsibility (OPR).

(2) Initial reports of suspected violations involving an employee of the Federal Bureau of Investigation (FBI) or the Drug Enforcement Administration (DEA), other than a law enforcement officer in paragraph (1), shall be submitted to the OPR in that component.

(3) In any other circumstance, initial reports of suspected security violations shall be submitted to the Office of the Inspector General (OIG).

(4) In all instances a copy of the initial report shall be submitted directly to the DSO.

c. If the OPR or the OIG, as appropriate, decline to investigate the violation, the component SPM shall complete the investigation of the incident. When the investigation has been completed, a final report shall be submitted to the DSO referencing the initial report and contain the following information:

(1) Any information required for the initial report that was not submitted previously;

(2) The name, position, social security number, date and place of birth, and date of the clearance of the individual(s) who were primarily responsible for the incident, including a record of loss, compromise, suspected compromise, or security violation for which the individual(s) previously had been determined responsible;

(3) A statement of the corrective action taken to prevent a recurrence of similar incidents;

(4) Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur;

(5) A damage assessment when appropriate; and

(6) Individual culpability reports as outlined below in Section 1.304.

1.304. Individual Culpability Reports.

Components shall establish and enforce policies that provide for appropriate administrative actions taken against employees who violate requirements of this Manual. They shall establish and apply a graduated scale of disciplinary actions in the event of employee violations or negligence. A statement of the administrative actions taken against an employee shall be included in a report to the DSO when individual responsibility for a security violation can be determined and one or more of the following factors are evident:

a. The violation involved a deliberate disregard of security requirements;

b. The violations involved gross negligence in the handling of classified material; or

c. The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness.

Chapter 2
Access to Classified Information

Section 1.
Requirements for Access

2-100. General Provisions.

a. No person may be given access to classified information or material originated by, in the custody, or under the control of the DOJ, unless that person:

(1.) Has been determined to be eligible for access in accordance with this manual,

(2.) Has a demonstrated need-to-know, and

(3.) Has signed a classified information non-disclosure agreement.

b. The Department Security Officer (DSO) may grant, deny, suspend, or revoke employee access to classified information pursuant to and in accordance with Executive Order (EO) 12968, as amended. The DSO may delegate the authority under this paragraph to qualified Security Programs Managers (SPMs) when the operational need justifies the delegation and when the DSO is assured that such officials will apply all access criteria in a uniform and correct manner in accordance with the provisions of EO 12968, as amended, and this manual. The fact that a delegation has been made pursuant to this section does not waive the DSO's authority to make**,** or override if necessary, any determinations that have been delegated.

c. The Adjudicative Guidelines in Annex C shall be used as the basis for determining eligibility for access to classified information and to sensitive compartmented information and special access programs. Eligibility shall be limited to U.S. citizens for whom an appropriate investigation of their personal and professional history affirmatively indicates loyalty to the U.S., 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. See 2-104 for an exception to the citizenship requirement. 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 U.S., and any doubt shall be resolved in favor of the national security.

d. 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 DOJ or any other personnel actions.

e. The DSO may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security.

f. The DOJ shall not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information. No negative inferences concerning the standards for access may be raised solely on the basis of the sexual orientation of the employee. Furthermore, no negative inference may be raised solely on the basis of mental health counseling. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards in subsection c. of this section are satisfied, and mental health may be considered where it directly relates to those standards.

g. 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.

2-101. Limitations on Access Eligibility.

a. Components shall keep the number of employees with access to classified information to the minimum necessary to perform official functions.

b. 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.

c. No person shall be granted access to specific classified information unless that person has an actual need-to-know for that classified information.

2-102. Temporary Access Eligibility. Based on a justified need, meeting the requirements of Section 3.3 of EO 12968, as amended, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication; however, temporary access may be terminated at any time based on unfavorable information identified in the course of the investigation.

2-103. Reinvestigation Requirements. Employees and contractors who are eligible for access to classified information shall be subject to periodic reinvestigations outlined in Annex D and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access.

2-104. Access by Non-United States Citizens.

a. Where there are compelling reasons in furtherance of the Departments' mission, immigrant alien and foreign national employees who possess a special expertise may, at the discretion of the DSO, 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 before access is allowed.

b. Exceptions to these requirements may be permitted only by the Attorney General (AG), the Assistant Attorney General for Administration (AAG/A), or designee to further substantial national security interests.

Section 2.
Financial Information Required

2-201. Release pursuant to the Fair Credit Reporting Act. Employees and applicants requiring access to classified information, and other individuals whose employment is in a position for which a background investigation (BI) by the DOJ is required, must sign a release pursuant to the Fair Credit Reporting Act (DOJ Form 555 (Revised Oct. 2008)), "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act." A Fair Credit Reporting Act release must be signed prior to the initiation of a BI. This release gives the DOJ the approval to obtain consumer/credit reports about the individual and is effective during the individual's tenure, or connection, with the DOJ.

2-202. Release Pursuant to Executive Order 12968, as amended.

a. Pursuant to EO 12968, as amended, a financial information release (Standard Form 713, "Consent for Access to Records") must be signed by an employee, as defined by 50 U.S.C. 436 et seq., prior to being granted access to classified information. The release shall be effective for such time as access to classified information is maintained and for a period of 3 years thereafter. The release permits the DOJ (or another authorized investigative agency), under the specific conditions identified below, to access the following information:

(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 as defined by 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.

b. Information may be requested pursuant to the E.O. 12968, as amended, Release in Annex B only under the following conditions:

(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 DOJ 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.

c. Under these limited conditions, the fact that an authorized investigative agency has requested or obtained information will not be disclosed to the employee or former employee to whom the information pertains.

2-203. Positions Requiring Financial Disclosure.

a. The AAG/A, in consultation with the Counsel for Intelligence Policy, shall designate each employee, by position or category where possible, who has a regular need for access to information that would reveal:

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

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

b. An employee may not hold a position designated as requiring a regular need for access to categories of classified information described above unless, as a condition of access to such information, the employee files with the DSO:

(1.) An approved financial disclosure form as part of all BIs or re-investigations;

(2.) An approved financial disclosure form, if selected by the DSO on a random basis; and

(3.) Reports all unofficial foreign travel to the DSO.

Section 3.
Obtaining Access Authorizations

2-300. General Procedures.

a. If there is not a current and appropriate BI on file or an appropriate BI currently being conducted, then the following is required:

(1.) The individual must be Livescan fingerprinted;

(2.) e-QIP SF-86 Questionnaire for National Security Positions;

(3.) When applicable, SF-86A, Continuation Sheet For Questionnaires SF-85, SF-85P, and SF-86;

(4.) When applicable, submit the Department's Foreign National Relatives or Associates Statement;

(5.) When applicable, a completed DOJ Form 555 needs to be submitted.

b. In rare instances when fingerprint charts must be submitted, components shall have procedures in place to ensure the person finger-printed does not have an opportunity to substitute the print charts prior to submission.

c. Each personnel and/or personnel security office authorized to initiate BIs, adjudicate investigative results, and grant employee access to classified information shall establish written procedures to accomplish these tasks.

2-301. Investigative Scope. The investigative scope for initial investigations and reinvestigations for each level of classified information is detailed in Annex D. Additional investigation may be required to obtain information relating to clearance eligibility requirements.

2-302. Duplication of Investigative Efforts. Investigations conducted by other U.S. Government Agencies shall not be duplicated when those investigations are current (within the last five years), are favorably adjudicated, and meet the scope and standards in Annex D for the level of access required. Prior to employment with the DOJ, a copy of the current investigation must be ordered. If reciprocity is denied, an FBI name and fingerprint check, DOJ 555 (Revised Oct. 2008), and updated SF-86 will be required on all new employees of the Department. If there is any doubt as to the adequacy of previous investigations, the DSO will make the final decision.

2-303. Access Reciprocity and Transferability. An access authorization granted by a U.S. Government agency or department to Government, military personnel or other individuals may be converted to a DOJ authorization at the same or lower level, subject to the following requirements:

a. The investigation upon which the authorization was issued is current and meets the standards established in Annex D for the level of access required;

b. If the time since the previous investigation exceeds the reinvestigation period standard, the access authorization may be issued, provided a new investigation has been initiated;

c. The DSO determines that no additional security processing is required;

d. No more than 24 months have passed since the termination date of the access authorization;

e. Complete form SF-86C if any information on prior SF-86 used for BI needs to be updated; and

f. No evidence of adverse information has arisen since the last U.S. Government investigation.

2-304. Concurrent Access. A concurrent access authorization may be requested if a component hires an individual or a consultant who has a current access authorization issued by another DOJ component. The component requesting the concurrent access shall not permit the individual access to classified information until clearance verification is received from the servicing personnel security office within the Department that access is authorized.

2-305. Downgrading Access. The component shall request the servicing personnel security office to administratively downgrade an access authorization when an employee no longer requires access to classified information at the existing level.

2-306. Terminating Access. The components must have procedures in place to ensure the servicing personnel security office is promptly notified to terminate an access authorization when an employee no longer requires access to classified information. Such notification procedures shall also apply when employment is terminated or there is a layoff or leave of absence for an indefinite period or for a period in excess of one year. The component shall advise the employee that access is being terminated because there is no current requirement for access to classified information and that termination of the access in no way reflects adversely on the employee or on future access eligibility. A security debriefing shall be provided as specified in Chapter 3 of this manual.

2-307. Reinstatement of Access.

a. Access authorizations that have been terminated may be reinstated at the same or lower level. The DSO will reinstate the access authorization without further investigation for an employee who was determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years provided:

(1.) They have remained a DOJ employee during the period in question;

(2.) The employee certifies in writing that there has been no change in the relevant information provided for the last BI; and

(3.) There is no information that would tend to indicate the employee no longer satisfies the standards for access to classified information.

b. The DSO will also re-approve access eligibility for individuals who have retired or otherwise separated from U.S. Government employment provided:

(1.) No more than 24 months have passed since termination of the access authorization;

(2.) A favorable adjudication of a BI completed within the prior five years;

(3.) An SF-86C is completed if any information has changed since completing the prior SF-86;

(4.) An FBI criminal records check (fingerprint check) reveals no unfavorable information; and

(5.) No evidence of adverse information has arisen since the last investigation.

2-308. Access Authorization Records. Personnel security offices shall maintain a current record of access authorizations granted. The record must include the level of access authorized, the date and type of the most current and any previous BIs and a record of any outstanding visit authorizations. A copy of each employees' executed Classified Information Nondisclosure Agreement (SF 312) shall be maintained separate from the employee's personnel security file. The personnel security office that grants the access shall maintain the SF 312 for a period of 70 years if it is kept separately from the employee's Official Personnel File (OPF) or 65 years if the SF 312 is maintained on the right side of the employee's OPF.

2-309. Facility Access Approvals. 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 to classified information, and access may be reasonably prevented. This section provides for "Facility Access Approvals" (FAA) when circumstances indicate an individual might inadvertently be exposed to classified information during the course of their duties. The FAA is not a security clearance or an authorization for access to classified information. It is a precautionary measure to reduce the risk of allowing uncleared persons to work in proximity of classified information. To grant the FAAs, the same investigative and adjudicative requirements established for the level of clearance is required. The Defense Security Service (DSS) is responsible for granting FAA under authority of the National Industrial Security Program (NISP). The Office of Information Safeguards and Security Oversight (OISSO) is a liaison with the DSS.

2-310. Funding Background Investigations. Components shall request sufficient funding each fiscal year to ensure that BIs and re-investigations of their employees requiring access to classified information are up-to-date.

Section 4.
Access by Persons Outside the Executive Branch

2-400. Conditions for Access.

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 DOJ 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 (FGI)).

c. Before such a release is made**,** the head of the Office, Board, Division, or Bureau making the release outside the Executive Branch shall determine the propriety of such action, in the interest of the national security, and must approve the release. Prior to the release, the DSO 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 manual.

2-401. Contractor Access. Personnel who are subject to a DOJ contract or grant and require access to classified information originated by or in the custody of the DOJ shall be processed for such access through the NISP. Under the NISP, the Department of Defense (DoD), DSS is responsible for arranging for the required investigations and administering the contractor clearances. Chapter 10 provides procedures for the establishment of a classified contract and how to obtain certification of a contractor's access authorization.

2-402. Legislative and Judicial Access. 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 DOJ. Federal Magistrate Judges must be determined eligible for access to classified information by the DSO pursuant to procedures approved by the AAG/A in consultation with the Judicial Conference of the United States. All other Legislative and

Judicial personnel including, but not limited to State and local Judges, Clerks of Court, judicial assistants, transcribers, interpreters, congressional staff, court reporters, typists, secretaries, law clerks, and translators who require access to classified information must be determined eligible by the DSO consistent with standards set out in this manual.

2-403. Others Requiring Access.

a. When other persons outside the Executive Branch who are not subject to the NISP require access to classified information originated by or in the custody of the DOJ, but do not otherwise possess a proper access authorization, an appropriate BI must be completed to allow the DSO to determine their eligibility for access to classified information.

b. The length of time it generally takes the FBI to complete a BI is 60-90 days. Therefore, all persons requiring access to classified information to participate in congressional or judicial proceedings should be identified and the BI initiated far enough in advance to ensure a minimum impact on such proceedings.

2-404. Need-to-Know Waiver.

a. The requirement that access to classified information may be granted only to individuals who have a need-to-know for the information may be waived for persons who are engaged in historical research projects or have previously occupied policy making positions to which they were appointed by the President.

b. All persons receiving access pursuant to this section must have been determined to be trustworthy by the DSO as a precondition before receiving access. Such determinations shall be based on such investigation as the DSO deems appropriate. Historical researchers and former presidential appointees shall not have access to FGI without the written permission from an appropriate authority of the foreign government concerned.

c. The DSO may grant waivers under this section if the SPM of the component with classification jurisdiction over the information being sought:

(1.) Makes a written determination that such access is consistent with the interest of national security;

(2.) Limits such access to specific categories of information over which the DOJ has classification jurisdiction;

(3.) Maintains custody of the classified information at a DOJ facility;

(4.) Obtains the recipient's written and signed agreement to safeguard the information in accordance with this manual and to authorize a review of any notes and manuscripts for determination that no classified information is contained therein; and

(5.) 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.

d. 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.

Section 5.
Denial or Revocation of Access

2-500. Denial Procedures.

a. Applicants and employees who are determined to not meet the standards for access to classified information must be:

(1.) Provided with a comprehensive and detailed written explanation of the basis for that decision as the national security interests of the U.S. 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 (2-500) 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.

2-501. Review of Denial or Revocation Determinations.

a. 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 section, whichever is later.

b. 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.

2-502. Appeal of Denials or Revocation.

a. Within 30 days of receipt of a determination under paragraph 2-501, the applicant or employee may appeal that determination in writing to the DOJ Access Review Committee (ARC), established under 28 CFR Part 17 § 17.15. The applicant or employee may request an

opportunity to appear personally before the ARC and to present relevant documents, materials, and information.

b. 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 DOJ 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.

c. 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 U.S., and any doubt shall be resolved in favor of the national security. Decisions of the ARC are final and conclusive and may not be appealed to the AG.

d. The DSO, or designee**,** 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 U.S. 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.

2-503. Limitations on Denial Procedures.

a. When the AG 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 U.S. by revealing classified information, the particular procedure shall not be made available. This is a discretionary and final decision not subject to further review.

b. This section does not limit the authority of the AG pursuant to any other law or EO to deny or terminate access to classified information if the national security so requires and the AG 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 DOJ 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.

Chapter 3
Security Education

Section 1.
Security Education and Training

3-100. General. This section establishes security education and training standards for all DOJ personnel authorized access to classified information, including original classification authorities, declassification authorities, security managers, security specialists, and all other personnel whose duties involve the creation or handling of classified information. Security Programs Managers (SPMs) may expand upon the coverage provided in this manual according to their component's needs.

3-101. Coverage. The component SPMs shall maintain a classified information training program that provides for initial and refresher training and termination briefings. The Department Security Officer (DSO) will assist the components in the development of the program. Security education and training should be tailored to meet the specific needs of the component's security program, and the specific roles employees are expected to play in that program. The component SPMs responsible for the program shall, in coordination with the DSO, determine the most effective methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, live classroom style instruction, on-line presentations, and other media and methods. Each component shall maintain records about the programs it has offered and employee participation in them.

3-102. Frequency. All DOJ personnel authorized access to classified information shall receive initial training on basic classified information security policies, principles and practices. Each component shall provide some form of refresher security education and training at least once annually in accordance with section 3-300 of this chapter.

3-103. Disclosure Warning. All DOJ personnel authorized access to classified information shall be informed in person by his or her immediate supervisor on an annual basis of their obligation not to disclose classified information to unauthorized persons and to report all contacts with persons who seek in any way to obtain unauthorized access to classified information. This requirement applies to all employees, including non-career employees who may be unaccustomed to handling classified information. The warning may be given during the annual job performance evaluation process.

Section 2.
Initial Training

3-200. Requirement. All DOJ personnel authorized access to classified information shall receive initial training on basic classified information security policies, principles, practices, and applicable criminal, civil and administrative penalties. The DSO shall provide the initial briefing unless this responsibility is delegated in writing to the component and their briefing has been approved by the DSO for use. Such training must be provided in conjunction with the granting of a security clearance and prior to accessing classified information. The initial briefing must include the training elements identified below.

a. Roles and responsibilities including:

(1.) the responsibilities of the senior agency official, component head, the SPM and the security specialist;

(2.) the responsibilities of employees who create or handle classified information;

(3.) whom should be contacted in case of questions or concerns about classification matters; and

(4.) the responsibility to submit the reports required in Chapter 1 of this manual.

b. Elements of classifying and declassifying information, including:

(1.) what is classified information and why it is important to protect it;

(2.) the levels of classified information and the damage criteria associated with each level;

(3.) the prescribed classification markings and why it is important to have classified information fully and properly marked;

(4.) the general requirements for declassifying classified information; and

(5.) the procedures for challenging the classification of information.

c. Elements of safeguarding, including:

(1.) the proper procedures for safeguarding classified information;

(2.) what constitutes an unauthorized disclosure and what are the penalties associated with these disclosures;

(3.) what are the general conditions and restrictions for access to classified information; and

(4.) what an individual should do when he or she discovers a possible compromise of classified information.

d. basic threat and counterintelligence information

3-201. Specialized Training. Original classification authorities, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive specialized training. This specialized training shall be provided upon the assumption of any of the positions listed above, and in the case of unavoidable circumstances must be received no later than six months after the assumption of any position listed above. The component SPM is responsible for providing this training with assistance from the DSO.

3-202. Original Classification and Declassification Authorities.

a. Original classification authorities (OCA) shall be provided detailed training on the proper application of classification and declassification decisions in accordance with Executive Order (EO) 13526 or its successor, with an emphasis on the avoidance of over-classification. Initial training for original classification authorities and persons with declassification authority shall include the following elements:

(1.) classification standards;

(2.) classification levels;

(3.) classification authority;

(4.) classification categories;

(5.) duration of classification;

(6.) identification and markings;

(7.) classification prohibitions and limitations;

(8.) sanctions;

(9.) classification challenges;

(10.) information sharing; and

(11.) security classification/declassification guides.

b. OCAs shall receive this training prior to originally classifying information. In addition to this initial training, OCAs shall also receive annual refresher training. OCAs who do not receive such mandatory refresher training within a calendar year shall have their classification authority suspended until such training has taken place.

c. The Attorney General (AG), Deputy Attorney General (DAG), or Senior Agency Official (SAO) 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 and reported to the DSO. Whenever such a waiver is granted, the individual shall receive the required training as soon as practicable.

3-203. Derivative Classifiers.

a. Individuals who apply derivative classification markings shall receive training the proper application of the derivative classification principles of EO 13526 or its successor, emphasizing the avoidance of over-classification. At a minimum this training shall cover the following elements:

(1.) the principles of derivative classification;

(2.) classification levels;

(3.) duration of classification;

(4.) identification and markings;

(5.) classification prohibitions and limitations;

(6.) sanctions;

(7.) classification challenges;

(8.) security classification guides; and

(9.) information sharing.

b. Derivative classifiers shall receive this training prior to derivatively classifying information. In addition to this initial training, derivative classifiers shall also receive annual refresher training. Derivative classifiers who do not receive such mandatory refresher training within a calendar year shall have their authority to apply derivative classification markings suspended until such training has taken place.

c. The AG, DAG, or SAO 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 and reported to the DSO. Whenever such a waiver is granted, the individual shall receive the required training as soon as practicable.

Section 3.
Annual Refresher Training and Termination Briefings

3-300. Annual Refresher Training. Component SPMs shall provide refresher training on an annual basis to all DOJ personnel authorized access to classified information. Refresher training should reinforce the classification, safeguarding and declassification policies, and the principles and procedures covered in the initial and specialized training. Annual refresher training should also address any policy updates and issues or concerns identified during component self-inspections. Each component shall maintain records of their refresher briefings and employee completion of the annual training.

3-301. Termination Briefings. Component SPMs shall ensure that each employee granted access to classified information who leaves the service of the DOJ receives a

termination briefing. Also, each DOJ employee whose clearance is withdrawn or revoked must receive such a briefing. At a minimum, termination briefings must impress upon each employee:

a. The continuing lifelong responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and

b. The obligation to return to the appropriate component official all classified documents and materials in the employee's possession.

3-302. SCI and SAP Refresher Training. Component SPMs shall provide specific SCI and SAP refresher training on an annual basis to all DOJ personnel authorized access to SCI or SAP information. Refresher training shall reinforce the basic classification, safeguarding, access, and reporting policies, and the principles and procedures covered in the initial SCI and SAP training. This refresher training should also address any current relevant concerns or policy updates. Each component shall maintain records of their SCI and SAP refresher briefings and employee completion of the annual SCI and SAP training.

Section 4.
Other Training Requirements

3-400. IT Security Training. IT security training is required for all persons involved in the management, use, or operation of systems which process classified or sensitive information. The training must ensure personnel are aware of their individual responsibilities for IT security and know how to fulfill these responsibilities. All computer systems users shall receive IT security training in accordance with Department CIO developed policies and standards.

3-401. Courier Briefing. Authorized couriers of classified information must be briefed on their responsibility to:

a. Ensure they possess written authority to escort or hand-carry classified information;

b. Ensure classified material is properly packaged (i.e., double-wrapped and sealed) and addressed;

c. Ensure classified material remains in their personal possession at all times and that the classified information is not read, displayed, or used in any manner in public places or on public transportation;

d. Ensure classified information is not left in hotel rooms, hotel safes, private residences, public lockers, etc;

e. Ensure that when traveling by Government or privately owned vehicle, classified information is not left unattended in the trunk or passenger compartment of the vehicle and is not stored in any detachable storage compartment such as a trailer or luggage compartment;

f. Ensure that when traveling by commercial aircraft within the U.S., classified information is transported in their carry-on luggage and Department of Homeland Security, Transportation Security Administration inspectors who do not ordinarily have security clearances, are not permitted to open envelopes or packages containing classified information;

g. Ensure that prior authorization is obtained from the DSO or the Department Special Security Officer for the transportation of SCI on commercial passenger aircraft within the U.S. and the transportation of classified information or SCI outside the U.S.;

h. Travel directly from the office sending the material to the destination;

i. Ensure the recipient of classified information has an appropriate security clearance and a need-to-know;

j. Ensure that classified material is not left with any person other than the intended recipient unless that individual's security clearance and authority to act as the recipient's agent is verified;

k. Ensure the recipient signs a classified document receipt for the material and the original of the receipt is returned to the sender;

l. Ensure that appropriate storage is available at the point of destination (i.e., GSA-approved security containers for classified information; approved facilities for SCI);

m. Ensure advance arrangements for proper overnight storage in a Government or a cleared contractor facility are made for trips involving overnight stopovers; and

n. Ensure a detailed description of the briefcase or other container is located at the courier’s workplace. In the event of an unforseen loss (theft or disaster), such a description will assist in the recovery of the information.

3-402. Foreign Travel Briefing. Employees authorized access to SCI must receive a defensive security briefing prior to foreign travel to high threat areas as stipulated in Chapter 11.

3-403. Additional Training. The DSO will develop additional security education and training according to program and policy needs.

Chapter 4
Classification Management

Section 1.
Original Classification

4-100. Classification Standards.

a. Information may be originally classified only if all of the following conditions are met:

(1) an original classification authority (OCA) 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 Executive Order (EO) 13526 (the Order); and

(4) the OCA 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 OCA is able to identify or describe the damage.

b. Should an original classification decision become the subject of a challenge or access demand, the OCA must be able to support the decision in writing, including identifying or describing the damage.

c. If there is significant doubt about the need to classify information, it shall not be classified.

d. Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

4-101. Classification Levels.

a. 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 that the OCA 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 OCA 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 OCA is able to identify or describe.

b. Except as otherwise provided by statute, no other terms shall be used to identify classified information.

c. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

4-102. Original Classification Authority.

a. Original classification means the classification of information in the first instance. The Attorney General (AG) is the DOJ's Top Secret OCA as designated by the President.

b. Top Secret OCA may only be exercised by the AG, the Assistant Attorney General for Administration (AAG/A), and officials to whom such authority is delegated in writing by the AG. No official who is delegated Top Secret classification authority pursuant to this paragraph may re-delegate such authority.

c. The AAG/A may delegate original Secret and Confidential classification authority to officials determined to have a demonstrable and continuing need to exercise such authority. No official who is delegated OCA pursuant to this paragraph may re-delegate such authority.

d. 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.

e. DOJ officials authorized to originally classify information at a specified level are also authorized to classify information at a lower level.

f. Delegations of OCA shall be in writing, identify the official by name or position, and the authority shall not be re-delegated. Delegations of OCA shall also be limited to the minimum required to administer the Order. The AG is responsible for ensuring that designated subordinate DOJ officials have a demonstrable and continuing need to exercise this authority.

g. Delegations of OCA shall be reported or made available by name or position to the Director of the Information Security Oversight Office (ISOO) on a frequency determined by the senior agency official (SAO), but at least annually.

h. Components shall limit requests for OCA to those positions that have a demonstrable and continuing need to exercise this authority. All component requests for OCA shall be submitted in writing to the Department Security Officer (DSO) and include the position for which classification authority is requested and justification for the request. OCA requests without proper justification may be

denied by the DSO. The DSO shall maintain a current listing of positions within DOJ with OCA.

i. All DOJ OCA's shall receive training in proper classification (including the avoidance of over-classification) and declassification annually. Such training must include instruction on the proper safeguarding of classified information and on the sanctions that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. OCA's who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the AG or the SAO until such training has taken place. A waiver may be granted by the AG, the Deputy Attorney General (DAG), or the SAO 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.

j. Whenever an employee, government contractor, licensee, certificate holder, or grantee of the DOJ who does not have OCA originates or develops information believed by that person to require immediate classification and safeguarding, and no authorized classifier is available, the person shall:

(1) Protect and safeguard the information in a manner appropriate for its classification level, consistent with the Order and its implementing directives;

(2) Apply the appropriate overall classification markings;

(3) Within five working days, securely transmit the information to the organization or DOJ component that has appropriate subject matter interest and classification authority;

(4) When it is not clear which organization or DOJ component would be the appropriate original classifier, the information shall be sent to the DSO to determine the appropriate organization; and

(5) The DOJ component with classification authority shall decide within 30 days whether to classify information.

k. Components shall maintain a record of all original classification actions including classification guides. The record shall include:

(1) the unclassified title and subject of the document or guide;

(2) the date and level of the original classification;

(3) the name and title of the OCA;

(4) the declassification date or exemption category, and

(5) any subsequent changes in the classification level or declassification date.

4-103. Classification Categories.

Information shall not be considered for classification unless the unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of the 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 (WMD).

4-104. Duration of Classification.

a. At the time of original classification, the OCA 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. An OCA shall follow the sequence listed in (a) (1), (2), and (3) of this section when determining the duration of classification for information originally classified.

(1) The OCA shall attempt to determine a date or event that is less than 10 years from the date of original classification which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

(2) If unable to determine a date or event of less than 10 years, the OCA shall assign a declassification date that is 10 years from the date of original classification decision.

(3) If unable to determine a date or event of 10 years, the OCA shall assign a declassification date not to exceed 25 years from the date of the original classification decision.

b. The only exceptions to the sequence in paragraphs (a) (1), (2), and (3) of this section are as follows:

(1) If an OCA is classifying information that could 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

(2) If an OCA is classifying information that could clearly and demonstrably be expected to reveal key design concepts of WMD, the duration shall be up to 75 years and shall be designated with the following marking, "50X2-WMD."

c. An OCA 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 the Order are followed.

(1) If an OCA does not extend the classification of information, the information is automatically declassified upon the occurrence of the date or event;

(2) If the date or event assigned by the OCA has not passed, an OCA 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;

(3) If the date or event assigned by the OCA has passed, an OCA may reclassify the information in accordance with the Order and its implementing directives only if it meets the standards for classification under sections 1.1 and 1.5 of the Order as well as section 3.3, if appropriate.

(4) In all cases, when extending the duration of classification, the OCA must:

(a.) Be an OCA with jurisdiction over the information;
(b.) Ensure that the information continues to meet the standards for classification; and
(c.) Make reasonable attempt to notify all known holders of the information.

d. No information may remain classified indefinitely. For information classified under prior orders or marked with X1 - 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, or in those cases where a document is missing a required declassification instruction or the instruction is not complete:

(1) A declassification authority, as defined in section 3.1(b) of the Order, may declassify it;

(2) An OCA with jurisdiction over the information may remark 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;

(3) 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.

e. All information classified under this section shall be subject to the automatic declassification provisions of this Manual if it is contained in records of permanent historical value under title 44, U.S.C.

f. An OCA may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures established in this Manual are followed.

4-105. 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 the Order;

(2) the identity, by name and position, or by personal identifier, of the OCA;

(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;
(b.) the date that is 10 years from the date of original classification;
(c.) the date that is up to 25 years from the date of original classification; or
(d.) in the case of information that could clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source "50X1-HUM" or key design concepts of WMD "50X2-WMD."

(5) a concise reason for classification that, at a minimum, cites the applicable classification category in section 1.4 of the 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 DOJ component originating the document shall indicate which portions are classified, with the applicable classification level, and which portions are unclassified.

d. 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.

4-106. 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 be reclassified after declassification and release to the public under proper authority only when the reclassification action is taken under the personal authority of the AG, or the DAG, who determines in writing, on a document-by-document basis that the reclassification of the information 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:

(a.) 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;

(b.) if the information has been made available to the public via a means such as Government archives or reading rooms, consideration is given to the 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

(c.) if the information has been made available to the public via electronic means, 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 the National Archives and Records Administration (NARA) and has been available for public use, reclassification requires notification to the Archivist and approval by the Director of the 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. 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 acknowledgment of this briefing.

(4) The reclassified information must be appropriately marked. The markings should include that authority for and the date of the reclassification action.

(5) All reclassification actions shall be forwarded to the DSO and classified or reclassified only at the direction of the AG, the DAG or the SAO. Reclassification actions must be reported to the National Security Advisor and to the Director of ISOO by the AG or SAO within 30 days.

d. Information that previously has not been disclosed to the public under proper authority may be classified or reclassified after the DOJ has received a request for it under the Freedom of Information Act (FOIA) (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Manual only if such classification meets the requirements of the Order and is accomplished on a document-by-document basis with the personal participation or under the direction of the AG, the DAG, or the SAO. The requirements in this paragraph also apply to those situations in which the information has been declassified in accordance with a specific date or event determined by an OCA in accordance with section 1.5 of the Order. When it is necessary to classify or reclassify such information, it shall be forwarded to the DSO via secure channels, and classified or reclassified only at the direction of the AG, the DAG, or the AAG/A as the SAO.

e. Classified information that has been declassified without proper authority, as determined by an OCA 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 through the DSO to the SAO who shall promptly provide a written report to the Director of ISOO.

f. Compilations of items of information that are individually unclassified may be classified if the compiled information reveals a new aspect of information that meets the criteria for classification. The information shall be referred to an OCA with jurisdiction over the information to make an original classification decision.

g. The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

4-107. Classification Challenges.

a. Authorized holders of information classified by the DOJ who in good faith believe that specific information is improperly classified or unclassified are encouraged and expected to challenge the classification status of the information pursuant to section 1.8 of the Order. Authorized holders may submit classification challenges in writing to the Department Review Committee (DRC), through the Office of Information Policy (OIP), United States Department of Justice, Washington, D.C. 20530. A formal challenge under this provision must be in writing, but need not be any more specific than to question 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 OCA for review and response.

c. The OCA shall promptly, and in no case later than 30 days, provide a written response to the DRC. The OCA may classify or declassify the information subject to challenge, or state specific reasons why the original classification determination was proper. If the OCA 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 OCA 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, it 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 its decision and a statement of his or her right to appeal that determination to the Interagency Security Classification Appeals Panel (ISCAP).

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 addressed in the mandatory review procedures of this chapter.

h. Whenever DOJ 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 DOJ is not required to process the challenge beyond informing the challenger of this fact and the challenger's appeal rights, if any.

i. 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 its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

j. The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such information inquiries are encouraged as a means of holding down the number of formal challenges and to ensure the integrity of the classification process.

k. Documents required to be submitted for prepublication review or other administrative processes pursuant to an approved non-disclosure agreement are not covered by this section, refer to Chapter 11, section 3 of this manual.

4-108. Classification Guides.

a. DOJ components with OCA shall prepare classification guides to facilitate proper and uniform derivative classification of information. These classification guides shall conform to standards contained in the Order, its implementing directives, and this Manual.

b. Each guide shall be approved personally and in writing by a DOJ official who:

(1) has program or supervisory responsibility over the information or the SAO; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

c. ISCAP approved exemptions from automatic declassification may be incorporated into classification guides, provided that the DSO and the ISCAP are notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

d. 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 could clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of WMD; and

(2) specific information incorporated into classification guides in accordance with section 2.2(e) of the Order.

e. Classification guides shall, at a minimum:

(1) identify the subject matter of the classification guide;

(2) identify the OCA by name and position, or personal identifier;

(3) identify a DOJ point(s)-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 25-year automatic declassification exemption codes listed in § 2001.26(a)(2), provided that:

(a.) the exemption has been approved by the ISCAP;
(b.) the ISCAP is notified of the intent to take such actions for specific information in advance of approval and the information remains in active use; and
(c.) the exemption code is accompanied with a declassification date or event that has been approved by the ISCAP.

f. Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information.

g. Original classification decisions shall be incorporated into classification guides as soon as practicable.

h. Originators of classification guides are encouraged to consult users of guides and other subject matter experts when developing or updating guides. When possible, OCAs are encouraged to communicate within the DOJ and with other organizations that are developing guidelines for similar activities to ensure the consistency and uniformity of classification decisions. 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.

i. Initial and updated guides shall be submitted to the DSO for written approval. The DSO shall ensure that a list of DOJ classification guides in use is maintained.

4-109. Fundamental Classification Guidance Review.

a. An initial fundamental classification guidance review shall be completed by every DOJ component with OCA no later than June 27, 2012. Fundamental classification guidance reviews will be conducted on a periodic basis thereafter, but shall be conducted at least once every five years.

b. The fundamental classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of the Order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of the Order. At a minimum, the fundamental classification guidance review shall focus on:

(1) Evaluation of content:

(a.) determining if the guidance conforms to current operational and technical circumstances; and
(b.) 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.

(2) Evaluation of use:

(a.) determining if the dissemination and availability of the guidance is appropriate, timely, and effective; and
(b.) 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. The fundamental classification guidance review shall include OCA's and component subject matter experts to ensure a broad range of perspectives. To the extent practicable, input may also be obtained from external subject matter experts and external users of the component classification guidance and decisions.

d. The AG shall provide a report summarizing the results of the fundamental classification guidance review to the Director of ISOO and shall release an unclassified version of this report to the public.

Section 2.
Derivative Classification

4-200. Use of Derivative Classification.

a. Derivative classification is the incorporation, paraphrasing, restatement or generation 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 also includes the classification of information based on a

classification guide. The duplication or reproduction of existing classified information is not derivative classification. 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 OCA.

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 classified 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 the 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, annually. Derivative classifiers who do not receive such training shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the AG, the DAG, or the SAO 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. Information assigned a level of classification will be considered as classified at that level 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.

Section 3.
Declassification and Downgrading

4-300. Authority for Declassification.

a. Information shall be declassified as soon as it no longer meets the standards for classification.

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 OCA;

(2) the originator's current successor in function, if that individual has OCA;

(3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has OCA;

(4) officials delegated declassification authority in writing by the AG or the SAO; or

(5) authorized users of ISCAP approved declassification guides.

c. 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, the declassification reviewing official shall refer the document with a recommendation for a decision to the DRC. The DRC shall review the document and make a recommendation to the AG or the SAO on whether the public interest in disclosure outweighs the damage to national security that reasonably might be expected from disclosure. The AG or SAO shall decide whether to declassify the information. This decision will be final. This provision does not amplify or modify the substantive criteria of procedures for classification or create any substantive or procedural rights subject to judicial review.

d. Prior to public release, all declassified records shall be appropriately marked to reflect their declassification

e. No information may be excluded from declassification 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.

f. Classified non-record materials, including artifacts, shall also be declassified as soon as they no longer meet the standards for classification.

4-301. Automatic Declassification

a. Classified records that have been determined to have permanent historical value under title 44, U.S.C., shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in 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. The Security and Emergency Planning Staff (SEPS), in coordination with component SPMs shall ensure that, subject to the exemptions described in this section, all originally classified information contained in records originated within their component records, that are 25 years old and have been determined to have permanent historical value under title 44, U.S.C., are reviewed for automatic declassification and other agency information identified for referral.

c. SEPS shall be responsible for coordinating with NARA and the Presidential Libraries to ensure that declassification is accomplished in a timely and efficient manner and in accordance with National Declassification Center (NDC) priorities. SEPS shall also establish DOJ policies and procedures to ensure the success of DOJ's automatic declassification program. This includes the establishment of a centralized DOJ Declassification Center.

d. DOJ Component heads with declassification responsibilities shall provide the appropriate resources to SEPS to ensure that the DOJ Declassification Center is properly staffed.

4-302. Exemption of Specific Information.

a. The AG or DOJ component OCA may propose to exempt from automatic declassification 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 WMD;

(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.

b. Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

c. At least 1 year before information is subject to automatic declassification, the respective DOJ component shall notify the AAG/A through the DSO of any specific information they propose to exempt from automatic declassification. The notification shall include:

(1) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(2) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(3) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

d. Proposed exemptions under this section, including classification/declassification guides which establish such exemptions, shall be forwarded to the DSO who with DRC coordination, shall recommend a disposition of the exemption request to the AAG/A. When the AAG/A determines the exemption is warranted, he or she will submit the request to the Director of ISOO, serving as Executive Secretary of the ISCAP.

e. The ISCAP may direct the DOJ component not to exempt the information or to declassify it at an earlier date than recommended. The AG or SAO may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

f. All records exempted from automatic declassification 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 WMD.

(2) In extraordinary cases, the AG or SAO 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 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 the AG or SAO, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the ISCAP.

4-303. File Series Exemptions.

a. Proposed file series exemptions shall be submitted to the DSO at least one year prior to the onset of automatic declassification. The DSO will coordinate proposed file series exemptions within DOJ and ensure that requests are forwarded to the ISCAP in a timely manner. File series exemptions should only be requested for records of 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 section 4-303. 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 ISCAP. Proposed file series exemptions shall include:

(1) a description of the file series;

(2) 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

(3) 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 WMD, 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.

b. The AG shall provide notification to the ISCAP of any file series that DOJ proposes to exempt at 25 years.

c. The ISCAP may direct the DOJ not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The AG may appeal such a decision to the President through the National Security Advisor.

d. File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending ISCAP review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

4-304. Integral File Blocks.

a. Classified records within an integral file block, 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. 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 DOJ requests an extension from the Director of ISOO on a case-by-case basis prior to December 31, 2011.

4-305. Special Media.

a. After consultation with the Director of the NDC and before the records are subject to automatic declassification, the AG or SAO 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.

4-306. Referrals.

a. 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. SEPS, through the DOJ Declassification Center, is responsible for overseeing the DOJ's referral process and coordinating with the NDC.

b. 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.

(1) In accordance with section 3.3(d)(3) of the Order, the identification of records eligible for referral 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, the DOJ 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) Records marked as containing RD or FRD or identified as potentially containing unmarked RD or FRD Data shall be referred to the DOE.

(4) 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 EO (rather than the Atomic Energy Act, as amended) must stand on its own merits.

(5) The SEPS DOJ Declassification Center, shall track and document referral actions and decisions in a manner that facilitates archival processing for public access. Documentation shall meet NDC requirements and all documentation on pending referral actions and referral decisions will be provided to the NDC when transferring records to NARA.

4-307. Temporary and Non-Records.

a. 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 components 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.

b. Classified information contained in temporary records and non-record materials is not subject to automatic declassification and shall be processed in accordance with section 3.6(c) of the Order.

4-308. Declassification Guidance to Contractors.

a. Classified information in the custody of contractors, licensees, certificate holders, or grantees. Pursuant to the provisions of the National Industrial Security Program, DOJ must provide security classification/declassification guidance to such entities or individuals who possess classified information. DOJ 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 DOJ 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.

4-309. Unscheduled Records.

a. 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.

4-310. Declassification Guides.

a. Declassification guides are the sole basis for continued classification of information after 25 years. Proposed declassification guides shall be submitted to the DSO, at least one year prior to the onset of automatic declassification for approval by the ISCAP. 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. Guides must be prepared to clearly delineate between the exemptions proposed under sections 3.3(b), 3.3(h)(1) and (2), and 3.3(h)(3) of the Order.

b. 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 AG or the designated SAO;

(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 EO 13526, state precisely the elements of information to be exempted from declassification to include:

(a.) The appropriate exemption category listed in section 3.3(b), and, if appropriate, section 3.3(h) of the Order; and

(b.) A date or event for declassification that is in accordance with section 3.3(b) or section 3.3(h) of the Order.

c. All DOJ ISCAP approved declassification guides shall be reviewed and updated as circumstances require, but at least once every five years. The SEPS DOJ Declassification

Center is responsible for maintaining a current list of declassification guides in use.

d. Declassification guides shall be disseminated within the DOJ to be used by all authorized personnel with declassification review responsibilities.

4-311. Exclusions from Automatic Declassification.

a. Restricted Data (RD) and Formerly Restricted Data (FRD) 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.

b. Any document marked as containing RD or FRD or identified as potentially containing unmarked RD or FRD shall be referred to the Department of Energy (DOE).

4-312. Systematic Declassification Review.

a. The DOJ 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 the Order. This includes individual records as well as file series of records.

4-313. Mandatory Declassification Review.

a. "Mandatory Declassification Review" (MDR) means the review for declassification in response to a request for declassification that meets the requirements of this section outlined below. Under this provision any person may request review of classified information for declassification.

b. All classified information shall be subject to a review for declassification if 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.

c. Records containing information exempted from automatic declassification in are still subject to the mandatory declassification review provisions of section 3.5 of the Order.

d. MDR requests for unclassified documents or previously classified documents that are declassified prior to the receipt of the request are not subject to a MDR review and may be denied by the receiving component. Additionally, documents in this category shall be considered non-responsive to an otherwise valid MDR request. Unclassified and Declassified documents must be requested under the provisions of the FOIA or the Privacy Act of 1974.

e. 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 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.

f. When the description of the information in a request is deficient, the component shall solicit additional identifying information 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. Requests for broad types of records, or similar non-specific requests may be denied for processing under this section.

g. Requests for mandatory review for declassification and any subsequent appeal to the DRC shall be submitted to the Director, Office of Information Policy (OIP), United States Department of Justice, Washington, D.C. 20530,describing the document or material containing the information with sufficient specificity to enable the DOJ component 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 to the DRC in the case of an appeal, and provide the requester with an acknowledgment of receipt of the request.

h. 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.

i. 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.

j. 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, the DRC, for administrative purposes, shall impose the burden of proof on the originating component to show that continued classification is warranted. 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. The DRC shall provide the requester with a written statement of reasons for its decision.

k. 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 the Order and rules issued by the ISCAP.

l. After a mandatory declassification 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. When information cannot be declassified in its entirety, the DOJ shall make reasonable efforts to release, consistent with other applicable laws, those declassified portions of the requested information that constitute a coherent segment. If the information, although declassified, is withheld, the requester shall be given a brief statement of the reasons for denial and a notice of the right to appeal the determination to the Director, Office of Information and Privacy, United States Department of Justice, Washington, D. C. 20530.

m. DOJ components shall conduct a line-byline review of the record(s) for public access and shall declassify information that no longer meets standards for classification. This information shall be released unless withholding is otherwise authorized and warranted under applicable law.

n. When a mandatory declassification review request for records in DOJ possession that were originated by another agency, the DOJ 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.

o. Fees. In responding to mandatory declassification review requests for classified records, DOJ components may charge fees in accordance with 31 U.S.C. 9701, relevant fee provisions in other applicable statutes, and Department of Justice MDR implementing regulations.

p. 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 (DOS), as appropriate, may consult with the foreign government(s) prior to declassification.

q. When a requester submits a request both under mandatory declassification review and the FOIA, the DOJ 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.

r. The DOJ 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.

s. The DOJ 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 EO 13526, 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 32 CFR § 2001.45(d).

t. Documents required to be submitted for prepublication review or other administrative process pursuant to an approved non-disclosure agreement are not covered by this section. Refer to Chapter 11, section 3 of this manual.

u. 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.

v. Regulations relating to the handling of mandatory declassification review requests, to include the identity of the person(s) or office(s) to which requests should be addressed, shall be published in the *Federal Register*.

4-314. Processing Requests and Reviews.

a. In response to a request for information under the FOIA, the Privacy Act of 1974, or the mandatory review provisions of the Order, or pursuant to the automatic declassification or systematic review provisions of the Order:

(1) DOJ may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified.

b. When DOJ 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, 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. In cases in which the originating agency determines in writing that a response under this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

c. The classification of information in records determined not to have permanent historical value or non-record materials, including artifacts, may be extended beyond the time frames established in sections 1.5(b) and 2.2(f) of the Order, provided:

(1) the specific information has been approved pursuant to section 3.3(j) of the Order for exemption from automatic declassification; and

(2) the extension does not exceed the date established in section 3.3(j) of the Order.

4-315. National Declassification Center (NDC).

a. The AG shall fully cooperate with the Archivist in the activities of the NDC 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 the Order, and

(2) upon request of the Archivist, assign personnel to the NDC who shall be delegated authority to review and exempt or declassify DOJ originated information contained in records accessioned into the National Archives, after consultation with subject-matter experts as necessary.

b. DOJ shall consult with the Director of the NDC concerning their automatic declassification program.

c. DOJ 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.

d. DOJ 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 DOJ that the records have been reviewed in accordance with Public Law 105-261, section 3161 governing RD and FRD.

4-316. Discretionary Declassification.

a. It is presumed that information that continues to meet the classification requirements of the 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. In accordance with section 3.1(d) of the Order and this Manual, the AG or DOJ SAO may declassify information when the public interest in disclosure outweighs the need for continued classification. This function is hereby delegated to all authorized DOJ original classification authorities and to all authorized DOJ declassification authorities, which includes those authorized officials within component agencies.

b. Officials exercising discretionary declassification pursuant to paragraph (a) shall be responsible for determining whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure.

c. DOJ components with OCA may establish a discretionary declassification program that is separate from their automatic, systematic, and mandatory review programs. Details of discretionary declassification decisions or special projects shall be maintained and reported to the DSO on an annual basis or as requested.

4-317. Classified Information in the Custody of Private Organizations or Individuals.

a. Authorized holders. The DOJ 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. DOJ 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.

4-318. Assistance to the Department of State.

a. Upon request, the DOJ shall assist the DOS 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. DOS Declassification Review Requests for the FRUS should be referred to the SEPS DOJ Declassification Center, who will coordinate declassification review with components, as appropriate.

4-319. Documents Accessioned to the Archives.

a. With SEPS assistance, each component shall, to the greatest extent possible, declassify information contained in records determined to have permanent historical value under Title 44 of the United States Code before they are accessioned into the NARA. Components shall cooperate with SEPS in carrying out an automatic declassification program involving accessioned DOJ records, Presidential papers, and historical materials under the control of the Archivist of the United States.

b. To the extent practicable, DOJ 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 the Order.

4-320. Foreign Government Information.

a. Foreign government information (FGI) shall retain its original classification markings or shall be assigned a United States classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. FGI retaining its original classification markings need not be assigned a United States classification marking provided that the responsible component determines that the foreign government markings are adequate to meet the purposes served by United States classification markings.

b. When foreign government information appears to be subject to automatic declassification, the declassifying agency (the agency that initially received or classified the information) 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 DOS, as appropriate, may consult with the foreign government prior to declassification.

Chapter 5
Marking Classified Information

Section 1.
Introduction

5-100. General.

a. A uniform security classification system requires that standard markings and other indicia be applied to classified information. Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Therefore, it is essential that all classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time that protection is required, the identity of the classifier, the source(s) for derivative classification, and any other notations required for protection of the information.

b. Except in extraordinary circumstances, the marking of classified information shall not deviate from the following prescribed formats, without the written permission of the Department Security Officer.

c. 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.

d. Since the primary purpose of classification markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure the necessary safeguarding.

e. Whenever practicable, a classified addendum shall be used when classified information constitutes a small portion of an otherwise unclassified document.

f. There are two types of classified information; that which is identified in the first instance as classified information, referred to as original classification, and that which is derived from existing classified sources, referred to as derivative classification. Within the DOJ, the vast majority of classified information is derivatively classified.

5-101. Mandatory Markings.

a. Every classified document shall be annotated, at a minimum, with three separate markings: portion markings, overall markings, and classification/declassification instructions. The markings for originally classified and derivatively classified information are somewhat different. The proper usage of each of these markings is described in detail throughout the rest of this chapter.

b. 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. An additional resource for marking guidance and marking examples is the Information Security Oversight Office (ISOO) Marking Classified National Security Information Booklet.

Section 2.
Original Classification Markings

5-200. Original Classification. Original classification is the initial determination that information requires protection against unauthorized disclosure in the interest of national security. Within the DOJ, only an individual authorized in writing by the Attorney General (AG) for Top Secret classification, or by the Assistant Attorney General for Administration for Secret and Confidential classification, may classify information in the first instance. An originally classified document must carry the following information:

a. Classification Authority;

b. Agency and office of origin;

c. Reason for classification;

d. Declassification instructions;

e. Overall classification marking;

f. Portion marking; and

g. Date of origin.

Section 5-201. Classification Authority. The name and position, or personal identifiers, of the original classification authority (OCA) shall appear on the "Classified By" line. An example might appear as:

Classified By: John Doe, Chief, Division 5
or
Classified By: ID#IMNO1

Section 5-202. Agency and office of origin. If not otherwise evident, the DOJ office of origin shall be identified and follow the name on the "Classified By" line. An example might appear as:

Classified By: John Doe, Chief, Division 5,
Department of Good Works, Office of Administration

Section 5-203. Reason for Classification. The OCA shall identify the reason(s) for the decision to classify. The OCA 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 Executive Order 13526 (the Order).

a. These categories as they appear in the Order are as follows:

(1.) Military plans, weapons systems, or operations;

(2.) Foreign government information;

(3.) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(4.) Foreign relations or foreign activities of the United States, including confidential sources;

(5.) Scientific, technological, or economic matters, relating to the national security;

(6.) United States Government programs for safeguarding nuclear materials or facilities;

(7.) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(8.) The development, production, or use of weapons of mass destruction (WMD).

b. An example might appear as:

Classified By: John Doe, Chief, Division 5,
Department of Good Works, Office of Administration
Reason: 1.4(g)

Section 5-204. 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 OCA will apply one of the following instructions:

a. 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: John Doe, Chief, Division 5,
Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20201014
or
Declassify on: Completion of Operation

b. 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: John Doe, Chief, Division 5,
Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20351010

c. If the classified information could clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, no date or event is required and the marking "50X1-HUM" shall be used in the "Declassify On" line.

d. If the classified information should clearly and demonstrably be expected to reveal key design concepts of WMD, no date or event is required and the marking "50X2-WMD" shall be used in the "Declassify On" line.

Section 5-205. Overall Classification Marking.

a. 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.

b. 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).

c. 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."

d. Each interior page of a classified document shall be conspicuously marked at the top and bottom either with the highest level of classification of information contained on the page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

e. Major components of complex documents are likely to be used separately. In such cases, each major component shall be marked as a separate document. Examples include: (a) each annex, appendix, or similar component of a plan, program or project description; (b) attachments and appendices to a letter; and (c)each major part of a report. If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and a statement included, such as: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method of marking is used, no further markings are required on the unclassified major component.

Section 5-206. Portion marking.

a. Each section, part, paragraph, or similar portion of a document containing classified National Security Information (NSI), 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.

b. To indicate the appropriate classification level, the symbols ''(TS)'' for Top Secret, ''(S)'' for Secret, and ''(C)'' for Confidential will be used.

c. Portions which do not meet the standards of The Order for classification shall be marked with ''(U)'' for Unclassified.

d. 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.

e. Illustrations, photographs, figures, graphs, drawings, charts, or similar portions contained in classified documents shall be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and shall be prominent and placed within or contiguous to such a portion. Captions of such portions shall be marked on the basis of their content.

f. Unclassified subjects and titles shall be selected for classified documents, if possible. A subject or title shall be marked with the appropriate portion marking symbol placed immediately preceding the subject or title.

g. A request for waiver from the portion marking requirement for a specific category of information shall be submitted through the component Security Programs Manager (SPM) to the DSO for submission to the Director of ISOO for approval. Requests shall include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden ordinarily will not be viewed as sufficient grounds to support a waiver.

h. A document not portion marked, based on an approved waiver, must contain a warning statement that it may not be used as a source for derivative classification.

i. If a classified document that is not portion marked, based on an approved waiver, is transmitted outside the originating organization, the document must be portion marked unless otherwise explicitly provided in the waiver approval.

Section 5-207. Date of origin. The date of origin of the document shall be indicated in a manner that is immediately apparent.

Section 3.
Derivative Classification Markings

Section 5-300. Derivative classification. All classified information shall be marked to reflect the source of the classification and declassification instructions. Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in section 2 of this chapter, 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. Documents shall show the following required information either on the cover, first page, title page, or in another prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation:

a. "CLASSIFIED BY" Line

b. "DERIVED FROM" Line

c. "DECLASSIFY ON" Line

Section 5-301. "CLASSIFIED BY" Line. The purpose of the "Classified By" line is to identify the derivative classifier of the document. 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: Jane Doe, Lead Analyst, Research and Analysis Division*
> or
> *Classified By: ID # IMN01*

Section 5-302. "DERIVED FROM" Line.

a. The purpose of the "Derived From" line is to identify the derivative classification applied to the material and the source document(s) or classification guide(s) under which it was classified. 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*

b. 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

c. 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. The derivative classifier shall include a listing of the source materials on, or attached to, each derivatively classified document.

Section 5-303. “DECLASSIFY ON” Line.

a. The purpose of the “Declassify On” line is to provide declassification instructions appropriate for the material. 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. 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.

b. 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.

c. 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), “X1 through X8", Manual Review (MR), or contains any other no longer valid declassification instruction, 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.

d. 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.

e. 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.

f. 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:

(1.) 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;

(2.) 25X1 through 25X9, with a date or event;

(3.) A specific declassification date or event within 25 years;

(4.) Absent guidance from an OCA with jurisdiction over the information, a calculated 25-year date from the date of the source document.

g. When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD.

h. Material containing Restricted Data (RD) or Formerly Restricted Data (FRD) shall not have a “Declassify On” line.

Section 5-304. 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 section 2 of this chapter.

Section 5-305. 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 section 2 of this chapter.

Section 5-306. 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.

Section 5-307. Date of origin. The date of origin of the document shall be indicated in a manner that is immediately apparent.

Section 4.
Marking in the Electronic Environment.

Section 5-400. Classification marking in the electronic environment. Classified NSI in the electronic environment shall be:

a. Subject to all requirements of the the Order.

b. 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.’’

c. 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.

d. Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the OCA. 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.

e. 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.

Section 5-401. Markings on classified e-mail messages.

a. 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.

b. 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.

c. A classified signature block shall be portion marked to reflect the highest classification level markings of the information contained in the signature block itself.

d. 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.

e. 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.

f. 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.

g. Unclassified e-mail messages transmitted on or prepared for transmission on classified systems or networks shall be clearly marked to indicate that they are UNCLASSIFIED in their entirety.

Section 5-402. Marking Web pages with classified content.

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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.

Section 5-403. 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:

http://www.center.xyz/SECRET/filename_(S).html
http://www.center.xyz/filename2_(TS).html
http://www.center.xyz/filename_(TS//NF).html

Section 5-404. Marking classified dynamic documents and relational databases.

a. 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.

b. 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).

c. 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.

d. Users developing a document based on query results from a database must properly mark the document in accordance with section 3 of this Chapter. If there is doubt about the correct markings, users should contact the database originating agency for guidance.

Section 5-405. Marking classified bulletin board postings and blogs.

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

Section 5-406. Marking classified wikis.

a. 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.

b. 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.

c. Wiki articles and entries shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

Section 5-407. Instant messaging, chat, and chat rooms.

a. 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.

b. 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.

Section 5-408. 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).

Section 5-409. Reserved.

Section 5.
Additional Requirements

Section 5-500. Documents Generated Under Previous Executive Orders. Documents classified under previous Executive Orders need not be re-marked to comply with the marking requirements of the Order. Classified material originated under previous Executive Orders may not have current required markings. If the source document does not contain portion markings, the overall classification of the source documents shall be used for the extracted information in the new document.

Section 5-501. Marking prohibitions.
a. Markings other than ''Top Secret,'' ''Secret,'' and ''Confidential'' shall not be used to identify classified NSI.

Section 5-502. Transmittal documents.

a. 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)*

b. If the transmittal document itself contains classified information, mark it as required for all other classified information, except:

(1.) Conspicuously mark the top and bottom of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures; and

(2.) mark the transmittal document with an appropriate instruction indicating its overall classification level when separated from its enclosures. For example:

> *Downgrade to Confidential when separated from Secret enclosures.*

Section 5-503. Foreign government information.

a. 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).''*

b. 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).''*

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.

Section 5-504. 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:

a. Released by the originator outside the originating activity;

b. Retained more than 180 days from the date of origin; or

c. Filed permanently.

Section 5-505. 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.

Section 5-506. 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.

Section 5-507. Classification by compilation. 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 OCA. 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.

Section 5-508. Approved dissemination control and handling markings.

a. 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.

b. 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.

c. If used, the dissemination control and handling markings will appear at the top and bottom of each page after the level of classification.

Section 5-509. Marking information that has been reclassified.

a. 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.

b. When taking this action, an OCA must include the following markings on the information:

(1.) The level of classification;

(2.) The identity, by name and position, or by personal identifier of the OCA;

(3.) Declassification instructions;

(4.) A concise reason for classification, including reference to the applicable classification category from section 1.4 of the Order; and

(5.) The date the reclassification action was taken.

c. The OCA shall notify all known authorized holders of this action.

Section 5-510. 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.

Section 5-511. Marking Miscellaneous Material. Material developed in connection with the handling, processing, production, and utilization of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and shall be destroyed at the earliest practical time, unless a requirement exists to retain such material. There is no requirement to mark such material, however it is recommended.

Section 5-512. Marking Training Material. Unclassified documents or material that are created to simulate or demonstrate classified documents or material shall be clearly marked to indicate the actual Unclassified status of the information. For example:

> *SECRET FOR TRAINING PURPOSES ONLY, OTHERWISE UNCLASSIFIED,*
> or
> *UNCLASSIFIED SAMPLE*, or a similar marking may be used.

Section 5-513. Marking Files, Folders or Groups of Documents. Files, folders, binders, envelopes, and other items containing classified documents, when not in secure storage, shall be conspicuously marked with the highest classification of any classified item included in the group. Cover sheets may be used for this purpose.

Section 5-514. Marking Microforms. Microforms contain images or text in sizes too small to be read by the unaided eye. The applicable markings shall be conspicuously marked on the microform medium or its container to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Further markings and handling shall be as appropriate for the particular microform involved.

Section 5-515. Marking Translations. Translations of U.S. classified information into a language other than English shall be marked to show the U.S. as the country of origin, with the appropriate U.S. markings and the foreign language equivalent.

Section 5-516. Marking Wholly Unclassified Material. Normally, wholly UNCLASSIFIED material will not be marked or stamped UNCLASSIFIED unless it is essential to convey to a recipient that the material has been examined specifically with a view to impose a security classification and has been determined not to require classification; or the material has been reviewed and has been determined to no longer require classification and it is declassified.

Section 5-517. Upgrading Action. When classified information is upgraded to a higher level, for example from Confidential to Secret, the new markings shall be immediately entered on the material accordingly, and all superseded markings shall be obliterated. The authority for and the date of the upgrading action shall be entered on the information.

Section 5-518. Inadvertent Release. If classified material is inadvertently distributed without the proper

classification assigned to it, or without any markings to identify the material as classified, the component SPM shall, as appropriate:

a. Determine whether all holders of the material are cleared and authorized access to it.

b. Determine whether control of the material has been lost and thus subject to compromise.

c. If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to the DSO via the Security and Emergency Planning Staff.

Section 6.
Declassification Markings

Section 5-600. General.

a. 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 John Doe, Chief, Division 5, August 17, 2008

Section 5-601. Marking information exempted from automatic declassification at 25 years.

a. When the Interagency Security Classification Appeals Panel (ISCAP) 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 WMD, 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 WMD, are exempt from automatic declassification at 50 years.

b. The pertinent exemptions, using the language of section 3.3(b) of the Order, are:

(1.) 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.

(2.) 25X2: reveal information that would assist in the development, production, or use of WMD;

(3.) 25X3: reveal information that would impair U.S. cryptologic systems or activities;

(4.) 25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5.) 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;

(6.) 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;

(7.) 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;

(8.) 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

(9.) 25X9: violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

c. The pertinent portion of the marking would appear as:

Declassify On: 25X4, 20501001

d. Documents should not be marked with a ''25X'' marking until the agency has been informed that the ISCAP concurs with the proposed exemption.

e. 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 ISCAP under section 3.3(j) of the Order.

f. 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 ISCAP approval to exempt foreign government information from declassification at 25 years. Upon receipt of ISCAP 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 ISCAP. 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.

Section 5-602. Marking information exempted from automatic declassification at 50 years.

a. 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 the AG, within five years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the ISCAP.

b. 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.''

c. When the information clearly and demonstrably could reveal key design concepts of WMD, the marking shall be ''50X2–WMD.''

d. In extraordinary cases in which the ISCAP 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.''

e. 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.

Section 5-603. Marking information exempted from automatic declassification at 75 years.

a. 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 ISCAP.

b. Information approved by the ISCAP 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.

Section 7.
Special Requirements for Restricted Data (RD) and Formerly Restricted Data (FRD) Documents

Section 5-700. Commingling of Restricted Data (RD) and Formerly Restricted Data (FRD) with information classified under the Order.

a. 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 this section, as well as the marking requirements in 10 CFR part 1045, *Nuclear Classification and Declassification*, must be followed.

b. Automatic declassification of documents containing RD or FRD is prohibited. Documents marked as containing RD or FRD are excluded from the automatic declassification 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.

c. For commingled documents, the ''Declassify On'' line 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 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.

d. If an RD or FRD portion is extracted for use in a new document, the requirements of 10 CFR part 1045 must be followed.

e. If a portion classified under the Order is extracted for use in a new document, the declassification date for the extracted portion shall be determined by using the source list, the pertinent classification guide, or consultation with the OCA 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.

f. 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 c. 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, the Atomic Energy Act, or 10 CFR part 1045 when they are requested under statute or the the Order.

Section 5-701. Transclassified Foreign Nuclear Information (TFNI).

a. 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.

b. 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. 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.

c. 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.

Section 5-702. Marking RD and FRD Documents.

a. RD classifiers shall ensure that each RD and FRD document is clearly marked to convey to the holder that it contains RD or FRD information, the level of classification assigned, and the additional markings in paragraphs b(3) an (4) of this section.

b. Front Marking. In addition to the overall classification level of the document, the following notices shall appear on the front of the document, as appropriate:

(1.) If the document contains RD:

RESTRICTED DATA

This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

(2.) If the document contains FRD, but does not contain RD:

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act of 1954.

(3.) An RD or FRD document shall be marked to identify the classification guide or source document, by title and date, used to classify the document:

Derived from:_____
(Classification Guide or source Document - title and date)

(4.) An RD or FRD document shall be marked with the identity of the RD classifier, unless the classifier is the same as the document originator or signer.

RD Classifier:_____
(Name and position or title)

c. Interior Page. RD Classifiers shall ensure that RD and FRD documents are clearly marked at the top and bottom of each interior page with the overall classification level and category of the document or the classification level and category of the page, whichever is preferred. The abbreviation "RD" and "FRD" may be used in conjunction with the document classification (e.g., SECRET RD or SECRET FRD).

d. Declassification Marking. DOJ declassification of documents containing RD or FRD is prohibited. Documents marked as containing RD or FRD are excluded from declassification 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.

Section 8.
Controlled Unclassified Information.

5-800. General.

a. Executive Order 13556, "Controlled Unclassified Information" was signed on November 4, 2010. Marking guidance regarding controlled unclassified information (CUI) will be incorporated into this section as it is developed by the Executive Agent.

Chapter 6
Safeguarding Requirements

Section 1.
General Requirements

6-100. General. Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification. This chapter describes the minimum requirements for safeguarding classified information.

North Atlantic Treaty Organization (NATO) classified 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 prescribed in Chapter 7 of this manual 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 manual.

6-101. Need-to-know Determinations. Organizational missions and personnel requiring access to classified information to perform or assist in authorized governmental functions shall be identified by component heads. These mission and personnel requirements are determined by the functions of a DOJ component 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. Classified information shall be disclosed only to persons with the appropriate access authorization and need - to-know.

6-102. Responsibilities of holders. 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 this manual; 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.

Section 2.
Standards for Security Equipment.

6-200. Storage.

a. Whenever new secure storage equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of the General Services Administration (GSA), and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

b. Only GSA approved security containers or DSO-approved open storage areas may be used for the storage of classified information. Information for procuring GSA-approved equipment may be obtained from component SPMs or the DSO. The standards for the construction of open storage areas are included in Annex F.

Section 3.
Storage of Classified Information

6-300. 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 approved by the DSO and 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.

6-301. Requirements for Physical Protection.

a. 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 section 8 of this Chapter. Refer to the DOJ COMSEC Manual for guidance on the physical protection of COMSEC material. In addition, supplemental controls are required as follows:

(1.) For GSA-approved containers, one of the following supplemental controls:
   (a.) Inspection of the container every 2 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 Attorney General (AG); 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.

(2.) 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.

(3.) For open storage areas not covered by Security-In-Depth, personnel responding to the alarm shall arrive within 5 minutes of the alarm annunciation.

b. 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 Attorney General (AG) 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 vault built to FED STD 832, one of the following supplemental controls is required:

(1.) Inspection of the container or open storage area every 4 hours by an employee cleared at least to the Secret level; or

(2.) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

c. 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.

6-302. Combinations.

a. 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.

b. A record will be maintained for each vault, secure room, or container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. Standard Form 700 (Security Container Information) will be used for this purpose. The SF 700 shall be stored in containers approved for the storage of classified information at the appropriate classification level, at the component SPM's office or in a separate container from the one storing the classified information. The SF 700 must be updated as prescribed in sub paragraph 6-302.c., and an outdated SF 700 must be destroyed when replaced. Access to the combination will be granted only to those individuals who are authorized access to the classified information that is stored inside.

c. 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:

(a.) Whenever such equipment is placed into use (manufacturers preset combination may not be used);

(b.) When any person having authorized knowledge of the combination no longer requires such knowledge;

(c.) When the possibility exists that the combination has been subjected to compromise;

(d.) When the lock is taken out of service (set back to standard combination 50-25-50, and pad locks to 10-20-30);

(e.) When any repair work has been performed on the combination lock; and

(f.) At least once every two years or sooner as dictated by the above events.

(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.

6-303. Key Operated Locks. When special circumstances exist, the Attorney General (AG) 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.

6-304. Repairs. The neutralization and repair of GSA-approved security containers and vault doors will be in accordance with FED STD 809.

Section 4.
Information Controls.

6-400. General. This manual establishes 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. Information management officials shall determine when such measures are appropriate for classified information in coordination with the Security Programs Manager (SPM).

6-401. 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 DOJ.

6-402. Reproduction.

a. 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.

b. Reproduction equipment capable of retaining images in an electronic storage device may be used only in accordance with procedures established in Annex I. Reproduction equipment which is not capable of retaining images may be approved for the reproduction of classified information by the SPM.

c. SPMs must ensure appropriate procedures for the reproduction of classified information are posted on or near equipment approved for such reproduction.

6-403. Forms. The use of standard forms prescribed in ISOO Implementing Directive 1, Subpart H is mandatory for all agencies that create and/or handle national security information.

6-404. Redaction.

a. Classified information may be subject to loss, compromise, or unauthorized disclosure if it is not correctly redacted. The Office of Information Policy (OIP) in coordination with the Department Security Officer (DSO) 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 Attorney General (AG) 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. Component heads shall ensure that personnel who perform redaction fully understand the policies, procedures, and methods and are aware of the vulnerabilities surrounding the process.

b. Technical guidance concerning appropriate methods, equipment, and standards for redaction of classified electronic and optical media shall be issued by NSA.

Section 5.
Transmission

6-500. 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 manual. Refer to the DOJ COMSEC Manual for safeguarding COMSEC material.

6-501. Dispatch. This manual establishes procedures which ensure that:

a. 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:

(1.) 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;

(2.) 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;

(3.) 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;

(4.) Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

(5.) When classified information is hand carried outside a facility, a locked briefcase may serve as the outer enclosure.

b. 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, the AG 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.

6-502. Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory.

a. 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.

b. Secret. Secret information shall be transmitted by:

(1.) Any of the methods established for Top Secret; U.S. Postal Service Express 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

(2.) The AG 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.

c. 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 street-side mail collection boxes is prohibited.

6-503. 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 no pass through a foreign postal system.

6-504. 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 section 6-503 of this Chapter 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.

6-505. Transmission by Courier.

a. Only DOJ personnel who have been appropriately briefed and have been specifically authorized in writing by the SPM may hand-carry classified information between their component and other organizations.

b. Employees authorized to be couriers will be briefed on their responsibilities. They will be required to sign an acknowledgment form stating that they have received the briefing and understand their responsibilities. Chapter 3 provides details on the required training elements for couriers.

6-506. Hand-carrying Classified Information on Commercial Aircraft.

a. Classified information shall not be hand-carried aboard commercial passenger aircraft unless:

(1.) There are no other authorized means available to move the information or accomplish operational objectives or contract requirements in a timely manner;

(2.) The hand-carrying has been authorized by the SPM; and

(3.) The hand-carrying is accomplished aboard a U.S. carrier.

b. Foreign carriers will be utilized only when no U.S. carrier is available and then the information must remain in the custody and physical control of the U.S. escort at all times.

c. Advance and continued coordination by the courier shall be made with departure airline and terminal officials and, where possible, with intermediate transfer terminals to develop mutually satisfactory arrangements. Specifically, a determination should be made beforehand as to where documentation will be required. Local Department of Homeland Security, Transportation Security Administration inspectors, can be of assistance in making this determination.

d. Individuals designated as couriers shall be in possession of a DOJ picture identification card and written authorization or official courier card issued from the SPM to carry classified information.

e. Couriers must receive a courier briefing as set forth in Chapter 3 of this manual and be knowledgeable of the provisions of this chapter.

6-507. Procedures for Hand-carrying Classified Information on Commercial Aircraft.

a. The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes or other suitable containers. Should such envelopes or pack ages be contained in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening and inspection for weapons.

b. Opening or reading of the classified document by the screening official is not permitted.

c. Under no circumstances will classified information or material be x-rayed.

d. Classified information in large sealed or packaged containers shall be processed as follows:

(1.) The DOJ official who has authorized the transport of the classified information shall notify the appropriate air carrier in advance.

(2.) The passenger carrying the information shall report to the affected airline ticket counter prior to boarding, present his documentation and the package or cartons to be exempt from screening. The airline representative will be requested to review the documentation and description of the containers to be exempt.

(3.) If satisfied with the identification of the passenger and his documentation, the airline official will be requested to provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection.

(4.) If the airline officials or screening personnel refuse to permit the package to be loaded onto the aircraft without inspection, the courier will contact the appropriate DOJ official for further instructions.

(5.) The actual loading and unloading of the information will be under the supervision of a representative of the air carrier; however, appropriately cleared personnel shall accompany the material and keep it under surveillance during loading and unloading operations.

6-508. Receipt of classified information. DOJ components 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 section 6-504 of this Chapter, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative is required.

Section 6. Destruction

6-600. General.

a. 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.

b. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with DOJ procedures and methods prescribed by this manual. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing (e.g., hammer mills, choppers, and hybridized disintegration equipment). DOJ components shall comply with the

destruction equipment standard stated in section 2 of this Chapter.

c. Pulpers, pulverizers, or cross cut shredders may be used only for the destruction of paper products. High wet strength paper, paper Mylar, durable-medium paper substitute, or similar water repellant type papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning shall be used to destroy these types of papers. Classified material in microform; that is, micro film, microfiche, or similar high data density material, may be destroyed by burning or chemical decomposition, or other methods approved by the DSO.

d. Prior to use, the component SPMs must approve the specific equipment, methods, and procedures for the destruction of classified information. The equipment and methods approved must be consistent with the standards established in this manual.

e. When crosscut shredders are used, they must meet National Security Agency, Central Security Services (NSA/CSS) specifications 02-01 and produce residue particle size not exceeding 1 mm in width and by 5mm in length. Existing fully operational crosscut shredders that meet the standard 1 /32 inch in width (with a 1/64 inch tolerance) by ½ inch in length can continue to be used until, such time as, the shredder requires replacement or a specific date for replacement is determined by the DSO.

f. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed.

g. The destruction of electronic media and information technology components is addressed in Annex G of this manual.

Section 7.
Loss, possible compromise or unauthorized disclosure.

6-700. 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.

6-701. 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, the DOJ 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.

6-702. Inquiry/Investigation and corrective actions. The AG 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.

6-703. Reports to ISOO. In accordance with section 5.59e0(2) of the order, the AG or senior agency official shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1),(2), or (3) of the Order that:

a. Is reported to oversight committees in the Legislative branch;

b. May attract significant public attention;

c. Involves large amounts of classified information; or

d. Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

Section 8.
Open Storage Areas.

6-800. General. This section describes the minimum construction standards for open storage areas. Open storage of classified documents requires DSO approval. Only areas that are constructed in accordance with Annex F and protected by an intrusion detection system meeting the standards of Annex G will qualify for such approval. All Open Storage Areas shall maintain a clean desk policy and all measures should be taken to respect the "need-to-know" requirement for access to classified information. Refer to the DOJ COMSEC Manual for the proper storage of COMSEC material.

6-801. 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.

6-802. 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 AG 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 AG.

6-803. 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.

6-804. Windows.

a. 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.

b. 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).

6-805. Restricted Areas. When it is necessary to control access to classified material in an area not approved for open storage, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority and shall safeguard the classified material at all times. All classified material will be secured during non-working hours in approved security containers, vaults or secured by using other methods approved by the DSO. A restricted area cannot be established for Sensitive Compartmented Information (SCI) information. SCI may only be discussed, processed and/or stored within a Sensitive Compartmented Information Facility (SCIF).

Section 9.
Office Procedures for Safeguarding Classified Information.

6-900. General. Each individual shall take all necessary precautions to prevent access to classified information by unauthorized persons (i.e., persons who do not possess an appropriate security clearance and need-to-know.)

6-901. During Working Hours. Precautions to be followed during normal working hours shall include:

a. Classified documents, when removed from storage for working purposes, shall be kept under constant surveillance and turned face-down or covered when persons who are not authorized access to the information are in the area. Cover sheets serve as a shield to protect classified information from inadvertent disclosure and to alert observers to the classification level of information attached. The following standard form (SF) classified cover sheets shall be utilized to cover classified documents:

(1.) SF 703, TOP SECRET Cover Sheet 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.

(2.) SF 704, SECRET Cover Sheet 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.

(3.) SF 705, CONFIDENTIAL Cover Sheet is affixed to the top of the Confidential document and remains attached until the document is destroyed.

b. Preliminary drafts, carbon sheets, computer media, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information shall be either destroyed by the person responsible for their preparation immediately after they have served their purposes, or shall be given the same classification and safeguarded in the same manner as the classified information they contain.

6-902. After Working Hours. SPMs shall ensure a system of security checks is implemented at the close of each working day to ensure that classified information is properly protected. Custodians of classified information shall conduct an inspection at the end of each work day to ensure:

a. All classified information, including computer media such as floppy disks used during classified processing sessions, is stored in approved security containers;

b. Waste material in burn bags, if utilized, are either stored in approved security containers or destroyed;

c. Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed;

d. Each security container used to store classified information shall be checked to ensure it is properly secured and documented on a SF 702 Security Container Check Sheet;

e. A record of the "end of day" check, SF 701 Activity Security Checklist (can be modified to accommodate unique requirements), shall be made and retained for a period of 30 days to facilitate the resolution of security incidents should they occur.

6-903. Security of Meetings and Conferences.

a. The official responsible for arranging or convening a conference or other meeting is also responsible for instituting procedures and selecting facilities which provide adequate security if classified information is to be discussed. The DSO can provide information on secure areas that may be used for classified meetings.

b. Meetings at which classified information is to be discussed will be held only in a U.S. Government cleared facility or at a cleared facility of a DOJ contractor or consultant. When necessary for the accomplishment of essential functions, a meeting involving classified information may

be held at another location provided it has been authorized by the DSO.

c. The official responsible for hosting the meeting or conference will notify each person present of any security limitations that must be imposed because of the level of access authorizations of the attendees or the physical security conditions of the facility. Additionally, the official responsible for the meeting will:

(1.) Ensure each person attending the classified portions of meetings has been authorized access to information of equal or higher classification than the information to be disclosed;

(2.) Ensure the area in which classified information is to be discussed affords adequate acoustical security against unauthorized disclosure;

(3.) Ensure that adequate storage facilities are available, if needed;

(4.) Control and safeguard any classified information furnished to those in attendance and retrieve the material or obtain receipts, as required; and

(5.) Monitor the meetings to ensure that discussions are limited to the level authorized.

6-904. Safeguarding Oral Discussions. Components shall ensure that all cleared personnel are aware of the prohibition against discussing classified information over unsecured telephones, cellular phones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons. Security managers should consider physical location as well as the capabilities of wireless devices and use sound judgment in developing appropriate security countermeasures against acoustic or electronic eavesdropping in classified work areas or where classified discussions may be held.

6-905. Emergency Plan for Safeguarding Classified Information. Components shall ensure an emergency plan is prepared for the safeguarding of classified information during an emergency of natural disaster that requires building evacuation. The emergency plan should provide for the protection, removal, or destruction of classified information, particularly for open storage areas.

Section 10.
Emergency Authorization for Disclosure.

6-1000. General. The Attorney General or designee may prescribe special provisions for the dissemination, transmission, safeguarding and destruction of classified information during certain emergency situations.

6-1001. Requirements for Emergency Disclosure. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, the Attorney General 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:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

b. Limit the number of individuals who receive it;

c. Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in Section 3, "Transmission Methods," of this Chapter, or other means deemed necessary when time is of the essence;

d. Provide instructions about what specific information is classified, 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;

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed non-disclosure agreement; and

f. 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:

(1.) A description of the disclosed information;

(2.) To whom the information was disclosed;

(3.) How the information was disclosed and transmitted;

(4.) Reason for the emergency release;

(5.) How the information is being safeguarded; and

(6.) A description of the briefings provided and a copy of the nondisclosure agreements signed.

Section 11.
Performance Ratings

6-1100. Requirements. The performance contract or other system used to rate employees shall include 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.

Chapter 7
Foreign Government Information

Section 1.
General

7-100. Definition. Executive Order 13526, "Classified National Security Information," defines "Foreign Government Information" (FGI) as:

a. 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;

b. 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

c. Information received and treated as "FGI" under the terms of a predecessor order.

7-101. Classification. FGI 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. FGI 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. Original classification authority is not required for this purpose.

7-102. Declassification. The declassifying agency is the agency that initially received or classified the information. When FGI 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.

7-103. Additional Requirements

a. Unless otherwise evident, documents that contain FGI 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 FGI be marked to indicate the government and classification level, using accepted country code standards, e.g., "(Country code-C)."

b. 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.

c. If the fact that information is FGI must be concealed, the markings described in this paragraph shall not be used and the document shall be marked as if it where wholly of U.S. origin.

d. Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government's security and classification instructions. In addition, they shall be marked on the front, "This Document Contains United States Classified Information." Portions shall be marked to identify the U.S. classified information, e.g., (US-S).

e. When classified records are transferred to NARA for storage or archival purposes, the accompanying documentation shall, at a minimum, identify the boxes that contain FGI; however, this requirement shall not apply if the fact that information is FGI must be concealed.

Section 2.
Safeguarding Requirements

7-200. General Safeguarding. Subject to more specific directives contained in this manual, FGI shall be protected, stored, transmitted, communicated, reproduced, and disposed of in the same manner as U.S. originated information of the same level of classification, unless more stringent safeguards are required as part of a treaty or condition of release by the foreign government that provided the FGI. When more stringent safeguards are required, they shall be stated in a cover sheet or memorandum attached to documents containing the FGI.

7-201. Storage of Foreign Government Information. FGI shall be stored and access shall be controlled generally in the same manner as U.S. classified material of an equivalent classification. The requirements described below are additional baseline safeguarding standards that may be necessary for FGI, other than North Atlantic Treaty Organization (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 United States Security Authority, NATO (USSAN) Instruction 1-07. To the extent practical, and to facilitate its control, FGI 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 FGI 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 FGI provided in confidence. In order to assure the protection of other FGI 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 FGI 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 FGI. 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 who have an established need-to-know, and where access is required by official duties 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 FGI to any third-country entity (including foreign nationals), or otherwise outside the Executive Branch, must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

7-202. Disclosure and Use Limitations. FGI is provided to the United States for specified purposes. FGI shall not be disclosed to nationals of a third country, or to any other third party, or be used for other than the purpose for which it was provided without the prior written consent of the originating foreign government.

7-203. Transfer within the United States. FGI shall be transferred within the U.S., its possessions, or territories, using the same channels and methods as specified by this manual for U.S. classified information of an equivalent classification except that non-cleared express overnight carriers shall not be used. The transfer of FGI to areas outside the U.S. shall be through government-to-government channels.

7-204. Reproduction. The reproduction of foreign government TOP SECRET information requires the written approval of the originating government. Records of such reproduction are required. Reproduction shall be limited to the minimum number of copies necessary. Reproduced copies of all foreign government information shall be controlled, protected, and accounted for in the same manner as the original version.

7-205. Disposition. FGI shall be destroyed when no longer needed unless the originating government has requested the return of the information. TOP SECRET FGI destruction must be witnessed and a destruction certificate executed and retained for 3 years. Destruction certificates are required for foreign government SECRET and CONFIDENTIAL information and shall be retained for 3 years. The destruction methods authorized for U.S. classified materials will be used for FGI materials of equivalent classification.

7-206. Loss, Compromise, or Suspected Compromise. The loss, compromise, or suspected compromise of foreign Government material shall be promptly reported to the Department Security Officer (DSO).

Section 3.
Foreign Disclosure of Classified U.S. Government Information.

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 government, 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 requirements on the medium containing the classified information. 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 authorizations.

Chapter 8
Information Assurance

Section 1.
Policy and Responsibilities

8-100. Information Assurance. Information Assurance is defined as the set of measures to protect and defend information and Information Technology (IT) systems by ensuring the availability, integrity, and confidentiality of information whether in electronic or hard copy format. This is accomplished through the integration of other security functions and processes that support the Departments Chief Information Officer (CIO) IT Security Program.

8-101. Policy.

a. Information shall be appropriately safeguarded at all times, including when used in Information Technology (IT) systems. Safeguards shall be applied such that

(1) individuals are held accountable for their actions;

(2) information is accessed only by authorized individuals and processes;

(3) information is used only for its authorized purpose(s);

(4) information retains its content integrity;

(5) information is available to satisfy mission requirements; and

(6) information is appropriately marked and labeled.

b. The security requirements identified in this chapter, DOJ Order 2640.2F, or its successor, or developed by the Department CIO shall be implemented to protect information that is captured, created, stored, processed, or distributed on IT systems. At a minimum all Department IT systems must posses security requirements such as accounts that uniquely identify each individual, as well as conforming to the Department's anti-virus, invalid attempt lock out, session inactivity, password, and audit policies. IT security requirements are identified in DOJ Order 2640.2F, or its successor. Controls are implemented using the following IT Security Standards, developed and approved by the Department CIO:

(1.) Access Control Family

(2.) Audit and Accountability Control Family

(3.) Awareness and Training Control Family

(4.) Certification, Accreditation, and Security Assessments Control Family

(5.) Classified Laptop and Standalone Computers Security Policy

(6.) Configuration Management Control Family

(7.) Contingency Planning Control Family

(8.) Identification and Authentication Control Family

(9.) Incident Response Control Family

(10.) Maintenance Control Family

(11.) Media Protection Control Family

(12.) Personnel Security Control Family

(13.) Physical and Environmental Protection Control Family

(14.) Planning Control Family

(15.) Risk Assessment Control Family

(16.) System and Communications Protection Control Family

(17.) System and Information Integrity Control Family

(18.) System and Services Acquisition Control Family

Additional standards may be developed by the Department CIO. Consult with the Information Technology Security Staff, Office of the DOJ CIO, for a complete listing of current standards.

c. Appropriate authorities, as defined in this chapter, shall be immediately notified of any threats, vulnerabilities, and incidents impacting systems that process their data. System vulnerability and incident reporting shall be consistent with IT Security Standard, Incident Response Control Family.

d. All IT systems are subject to monitoring consistent with applicable laws and regulations, and as provided for by DOJ policies, procedures, and practices. As a minimum, monitoring will assess the adequacy of the confidentiality, integrity, and availability of controls.

e. All DOJ IT systems that process, store or handle Department information shall be certified and accredited in accordance with the requirements stated in this chapter and following the policies, standards, direction, and guidance provided by the Department CIO.

8-102. Assignment of Responsibilities. A clearly defined structure will assist DOJ Component Heads and/or designees in implementing the DOJ IT Security program and ensuring its integration with other aspects of the DOJ's security programs for the protection of classified information.

8-103. DSO Responsibilities. The DSO is responsible for:

a. Development and administration of Department- wide security policy and programs, except for those areas that are within the responsibility of the Department CIO under DOJ Order 2640.2F, Information Technology Security, or its successor.

b. Conducting security compliance reviews to assess the overall effectiveness of security program implementation across the Department, including IT security.

c. Ensuring the development and implementation of Department-wide policies and procedures that govern: TEMPEST; Technical Surveillance Countermeasures (TSCM); Personnel Security; Physical and Environmental Security; Storage and Marking; Media Disposal; Media Reuse; Communications Security (COMSEC); facsimile security; copier security.

d. Responsible for the DOJ Sensitive Compartmented Information (SCI) program for Department entities not part of the Intelligence Community (IC), to include obtaining accreditation of IT systems processing SCI from the Director, Central Intelligence Agency (CIA).

8-104. DOJ CIO Responsibilities. The DOJ CIO is responsible for:

a. Directing and providing integrated security policy for the DOJ Information Technology Security Program, as set forth in DOJ Order 2640.2F or its successor.

b. Ensuring the development and implementation of Department wide policies and procedures that govern the Certification and Accreditation process, incident response capability, IT security training, and technical controls.

c. Monitoring IT security related activities to verify and validate the effective implementation of system and program IT security controls.

8-105. Component Security Program Manager (SPM) Responsibilities. The IT security responsibilities for the Component SPM as delineated in DOJ Order 2600.2C, Security Programs and Responsibilities, or its successor, may be delegated by the Component Head to the Component's CIO, if applicable, for the establishment and management of the Component's IT security program. If the IT security role of the SPM is delegated, as a minimum and in addition to those duties outlined in DOJ Order 2600.2C, the SPM shall still be responsible for:

a. Ensuring compliance with the provisions of this chapter.

b. Reviewing and approving security plans for classified IT systems and reviewing classified IT procurement requests to ensure physical, personnel, and administrative security policies are being adhered to.

c. Maintaining coordination and liaison with the DSO, Department CIO, and Component CIO in the implementation of security programs and in making recommendations for changes of security policies, and procedures as it relates to the protection of classified and SBU information.

Section 2.
Minimum Security Requirements

8-200. General. All IT systems processing classified information, including those located overseas, shall meet the requirements of this chapter and Department CIO developed IT security policies and standards.

a. Components may impose more stringent requirements.

b. IT Systems that process National Security Information shall conform to policy promulgated by the Committee on National Security Systems.

c. IT systems that process Sensitive Compartmented Information (SCI) shall conform to the provisions of Intelligence Community Directive (ICD), 503.

8-201. Accreditation.

a. IT systems must be certified and accredited following the standards, direction, and guidance provided by the Department CIO.

b. All IT systems that process, store, or transmit SCI, for Department entities which are not part of the IC, shall be coordinated with the DSO and the Department CIO prior to development and authority to operate which shall be granted by the CIA.

8-202. Media Storage. All media must be protected in accordance to the provisions set forth in the manual for all sensitive information, to include Chapter 6.

8-203. Marking and Labeling. Markings on hardware, output, and media containing classified information shall be marked in accordance with this section and Chapter 5 of this manual.

8-204. Review of Output and Media.

a. Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application.

b. An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

c. Human review of information has to meet two criteria to be sufficient: a review of the information content to validate the actual classification level of the data, and a review of embedded or hidden information that is part of the data. Information in its presentation form does not always show embedded or hidden data. This data may require a different process or application (or tools) to reveal the hidden data for the human review.

d. Tools may be used to aid the individual during the review process. Automated tools can aid in the review of large amounts of data. A review of data is more reliable if it includes both a human review and review using automated tools. Reviews should not rely solely on an automated review unless the automated review process is approved by the appropriate Designated Approving Authority (DAA).

e. Because a human is interacting with automated processes to conduct reviews, the information being reviewed should have an integrity feature so that the review process does not alter the information being reviewed. For example, write protect media before the information review.

8-205. Media Release

a. IT systems that have processed, stored, or transmitted classified information shall not be released from a component's control until the equipment is sanitized.

b. Department IT equipment under maintenance warranty contracts shall include stipulations that equipment removed from the Department's physically protected offices shall be sanitized before its removal.

c. The security inspection and release form or similar documentation, attached in Annex G, shall be used to document the release or disposal of any IT system or processing component.

8-206. Media Accountability. Media accountability shall be implemented that provides a set of protection mechanisms comparable to those required for equivalent paper documents.

8-207. Media Disposal.

a. Media consists of any substance upon which information is recorded by a computer. Disposition procedures for media used to process or store classified or sensitive information must be identified in the security plan.

b. Classified IT system media must be protected and marked in accordance with Chapter 5 and Section 8-205 of this manual and classified media shall be properly protected until declassified or destroyed.

c. Due to the rapidly changing nature of computer media, and threats to the media, the specific method used to purge or destroy media must be approved in writing by the SPM. The SPM, in consultation with the DSO, must consider the most current threats to the specific media when approving destruction methods, which shall meet Department requirements. Specific guidance for the purging, declassification, disposition, or destruction of media is available from the DSO. The general destruction methods are listed below. Annex G provides guidance to assist in the selection of destruction methods.

(1) When no longer usable, diskettes, tape cartridges, hard drives, and other media used to process SBU and classified information may be degaussed with the appropriate National Security Agency (NSA) approved degausser. Consult the current NSA Degausser Products List to determine the appropriate degausser. If degaussing equipment is used, the Information System Security Officer (ISSO) shall establish procedures to ensure strict compliance with the manufacturer's instructions for the operation and continued effectiveness of the equipment.

(2) Magnetic floppy disks containing classified and sensitive information may also be destroyed by burning or shredding. Crosscut shredders, which meet the requirements set forth in Chapter 6, section 201 and 600 of this manual may be used to destroy magnetic floppy disks that have been removed from the protective covering.

(3) The security inspection and release form or similar documentation, attached in Annex G, shall be used to document the release or disposal of any IT system or processing component.

8-208. Media Reuse. When no longer required for mission or project completion, IT storage media that will be re-utilized by another person within the component shall be overwritten with Department CIO approved software or degaussed as appropriate. The media shall be protected consistent with the data sensitivity and/or at the highest classification level at which they were previously used, unless the media has been properly sanitized by using the appropriate NSA approved degausser. The degaussing of hard disks may cause damage (i.e., loss of timing tracks and servo motors), which may prohibit their continued use. The procedures shall be documented in the system security plan.

8-209. Communications Security (COMSEC). The conduct of all DOJ COMSEC activity, including the acquisition of COMSEC products, shall be in accordance with this manual; as well as the DOJ COMSEC Manual. The DOJ COMSEC Manual implements the national policy as set forth in the Committee on National Security Systems (CNSS) Instruction 4005, “Safeguarding Communication Security (COMSEC) Facilities and material”.

a. COMSEC shall be implemented to be commensurate with the highest classification or sensitivity level of the information transmitted. When classified information

transits an area not under access controls as stringent as required for that classification, it will be protected by encryption or a protected distribution system (PDS) approved by the DSO.

b. Encryption, using equipment and keying material approved by the NSA, Type 1 is required for all classified communications. COMSEC for classified information shall comply with all applicable NSA and DOJ policies. The DSO shall monitor compliance with these requirements.

c. COMSEC incidents shall be immediately reported in accordance with the DOJ COMSEC Manual.

8-210. Personnel Security Requirements

a. Employees and non-DOJ personnel, including contractors, shall have access authorizations commensurate with the highest level of information processed by the IT systems they access. In unusual circumstances, the SPM may make exceptions to this requirement provided the uncleared person is monitored by a knowledgeable escort with the appropriate access authorization. The escort shall be responsible for ensuring the escorted person does not access sensitive or classified information for which he or she is not cleared.

b. Personnel with IT system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IT system. Duties, responsibilities, privileges, and specific limitations of IT users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the IT system.

c. Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems, unless a waiver has been granted by the Head of the Component, with the concurrence of the DSO and the CIO.

d. All personnel granted unescorted physical access to an area containing classified IT systems shall have an appropriate security clearance.

e. Department CIO guidance regarding personnel security for IT systems can be found in IT Security Standard, Personnel Security.

8-211. Physical Security. Classified information shall only be processed at facilities approved by the Federal Government for processing of classified information. Approval must be for the processing of classified information at or above that which is being processed. Facilities that house IT systems must include:

a. Protection against the unauthorized disclosure, destruction, or modification of IT hardware, software, documentation, and all classified and sensitive information handled by the IT system. The level of control and protection will be commensurate with the maximum classification or sensitivity of the information present in the IT system.

b. Protection of IT system hardware, software, or documentation if access to such resources would reveal information that may be used to eliminate, circumvent, or otherwise render ineffective the security safeguards of the system.

c. Safeguards that prevent or detect unauthorized access to the IT system and unauthorized modification of the IT system hardware and software. Hardware integrity of the IT system, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IT system.

d. An open storage area constructed in accordance with Annex E and approved in writing by the DSO. The DSO must be consulted in all phases of selection, design, and modification of open storage areas. Processing of classified information in a non approved open storage area must be in accordance with Chapter 6-805, Restricted Areas.

e. For SCI IT systems, a Sensitive Compartmented Information Facility (SCIF) in accordance with Chapter 11 of this manual.

f. Fire and water protection for IT facilities and any room housing media libraries.

g. Positioning of devices that display or output classified information in human-readable form to prevent unauthorized individuals from reading the information.

h. Department CIO guidance regarding physical security for IT systems can be found in IT Security Standard, Physical Security.

8-212. TEMPEST.

a. Committee on National Security Systems Policy No. 300, National Policy on Control of Compromising Emanations, establishes national TEMPEST policy for national security systems

b. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 7000, TEMPEST Countermeasures for Facilities, shall be used to determine applicable TEMPEST countermeasures for IT systems processing classified information.

8-213. Technical Security Countermeasures (TSCM). The components of IT systems, associated data communications, and networks shall be protected in accordance with national TSCM policies and procedures applicable to the sensitivity level of the data being transmitted. Contact the DSO for the appropriate procedures to request a TSCM survey.

8-214. Facsimile Security.

a. All classified and sensitive facsimile transmissions shall be preceded by a cover sheet containing the following information:

(1) The classification or sensitivity of the information.

(2) The name, office and voice/fax telephone numbers for the recipient(s) and sender.

(3) A warning banner with instructions to the recipient if the facsimile was received in error.

b. Classified information shall be encrypted for transmission with National Security Agency (NSA)-approved encryption.

8-215. Digital Copiers

a. Devices that have the capability to store information in their internal memory for processing, such as digital copiers and facsimile machines, are considered IT systems and are therefore subject the requirements set forth in this manual and all other Department IT security standards**.**

b. Reproduction of classified information with multi function digital copiers shall be in accordance with Section 6-402 and Annex I of this manual.

Section 3.
Additional Provisions

8-300. Acquisition of IT Products for Classified Purposes.

a. All IA or IA-enabled IT hardware, firmware, and software components or products (to be used on IT systems entering, processing, storing, displaying, transmitting National Security Information) incorporated into DOJ IT systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11.

b. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program. For a listing of evaluated products go to http://www.niap.nist.govhttp://www.niap-ccevs.org/cc-scheme/vpl/.

8-301. IT Security Training. All classified IT systems users must receive the training specified in Chapter 3 of this manual and in accordance with Department CIO developed policies and standards.

8-302. Security Incident Reporting. All IT security incidents must be handled in accordance with Section 1-302 of this manual.

8-303. Maintenance. IT systems are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.

a. Cleared Maintenance Personnel. Maintenance personnel who are cleared to the highest classification level of information on the IT system and indoctrinated for all information processed on that system do not require an escort, if need-to-know controls can be implemented. When possible, an appropriately cleared and technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that security procedures are being followed.

b. Uncleared (or Lower-Cleared) Maintenance Personnel.

(1) If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.

(2) System initiation and termination shall be performed by the escort. In addition, keystroke monitoring may be performed during access to the system.

(3) Prior to maintenance, the IT system/component shall be completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When an IT system/ component cannot be cleared, procedures shall be enforced to deny the maintenance personnel visual and electronic access to any classified data contained on the IT system.

(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY".

8-304. Employee Owned Systems. Employee-owned systems SHALL NOT be used for processing classified information.

8-305. Portable Electronic Devices. Portable Electronic Device (PED) is a generic term used to describe the myriad of small electronic devices that are widely available. PEDs include: SME/PEDS, laptops, personal digital assistants, palm

tops, hand-held computers and workstations, cell phones, two-way pagers, wireless email devices, two-way radios, devices with audio/video/data recording & playback features, watches with communications and synchronization capabilities.

a. The introduction of classified information to an unauthorized PED will result in a security violation. If this occurs the PED needs to be controlled as classified material.

b. Requirements for introducing PEDS in or out of classified facilities are as follows:

(1) PEDs, hardware/software associated with them, and media must be controlled when entering/exiting a SCIF or areas where classified processing is authorized.

(2) PEDs are prohibited from operating within a SCIF or areas where classified processing is authorized, unless approved by the agency granting the SCIF and/or classified processing facility.

(3) Connection of a PED to any IT system within a SCIF or an approved classified processing facility must be approved by the ISSO and SCIF Control Officer or facility supervisor in writing, and in coordination with the Department CIO and DSO.

c. Specified PEDs (i.e. Laptop/Notebook Computers) may be used to process classified information. In addition, these PEDs may be granted approval to connect to IT systems on a case-by-case basis in writing by the ISSM. Specified PEDs approved to process classified information must meet minimum security requirements issued by the Department CIO as well as this manual, including Annex H.

d. Lost or stolen PEDs must be reported immediately to the Security Program Manager (SPM) and the Property Management Officer. If the PED contained classified information, the SPM shall provide written notification to the Department Security Officer in accordance with Chapter 1 of this manual. The originating office must document the circumstances surrounding the loss/theft to include a complete damage assessment regarding possible compromise of sensitive data.

8-306. Multi-Position Switches. Only Key Board/Video/Mouse (KVM) or Key Board/Monitor/ Mouse (KMM) Switches which are appropriately approved shall be used when sharing a Key Board, Video Monitor or Mouse between Central Processing Units (CPU) at different classification levels.

a. The use of switch boxes for print services between classification levels is prohibited. Switch boxes may be used between the same classification levels for print services.

b. The introduction and use of multi-position switches in a classified environment presents a moderate degree of risk to classified or sensitive information and systems. Therefore, all users will be responsible for the management of these devices. To minimize the risk of inadvertently entering information onto the wrong network, the following requirements must be met.

(1) All components of the IT system must be labeled in accordance with DOJ policy and this manual.

(2) To avoid inadvertent compromises, systems joined by multi-position switches will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the banner background will be in a solid color that matches the classification (SCI - yellow, Top Secret - orange, Secret - red, Confidential - blue, Unclassified - green). When systems have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

(3) Screen Lock applications must display the maximum classification of the system on which the system is currently logged into and shall implement a lockout feature to re-authenticate the user.

(4) Switches that support "Hot-Key" capability to switch, toggle or otherwise affect the switching between CPUs are prohibited.

(5) Switches with the ability to automatically scan and switch to different CPUs are prohibited.

(6) Systems using KVM/KMM switches must not use keyboards or mice with wireless or infrared technology

(7) At a minimum, users must ensure that they use different/unique passwords for each system connected through a multi-position switch. Whenever possible, system administrators should employ different logon USERIDs to help users further distinguish between the systems.

(8) Data of a higher classification shall not be introduced to a system of a lower classification.

8-307. Processing at Different Sensitivity Levels Utilizing Removable Hard Drives. IT workstations and/or laptops with removable hard drives can dedicate separate hard drives for classified and unclassified processing providing the following requirements are met.

a. The system shall be validated to ensure that information does not reside on any component of the system once the hard drive is removed and that the system does not have the capability to retain information once the hard drives are removed.

b. Volatile memory components are cleared (usually by powering the system down).

c. The IT system must be shut down before the removable media is exchanged.

d. Nonvolatile memory components which are significant components of a system could retain information between the different processing periods. When relying on removable media, the system shall have no significant nonvolatile memory components which could contain unauthorized information remaining within the system.

(1) Any system approved for utilizing removable hard drives processing at different sensitivity levels will be prohibited from containing nonvolatile memory or a fixed hard drive.

(2) If applicable, the system may have a single accreditation according to the highest sensitivity and the most restrictive data processed on all of the removable drives.

e. To avoid inadvertent compromises, removable hard drives used on IT systems for unclassified and classified processing will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the banner background will be in a solid color that matches the classification (SCI - yellow, Top Secret - orange, Secret - red, Confidential - blue, Unclassified - green). When removable hard drives have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

f. The removable drives will be properly labeled and stored according to the provisions of this chapter.

g. The use of removable hard drives on an IT system authorized for classified and unclassified processing shall be documented in its systems security plan.

h. IT workstations and/or laptops with removable hard drives processing at different sensitivity levels will require creating a new label for the shell to indicate that the computer is authorized to process classified or unclassified information provided that the requirements of this section is adhered to.

8-308. Introduction of Classified Information. Classified information will not be introduced into an IT system until the data classification and sensitivity of the IT system has been determined. Data will not exceed the security classification level for which the IT system is approved to operate. If the IT system configuration includes non removable hard disks that store classified material, the entire system must be stored, when left unattended in an area approved for the storage of the highest classification of information the system is authorized to process.

8-309. Docking stations. Computers connected to networks via a docking station shall adhere to the accreditation level of the network they are accessing. The IT system will be protected at a level determined by the system designation of the IT system being accessed. The use of docking stations shall be approved by the DAA of the IT system being accessed. Computers utilizing docking stations shall not connect to systems with differing classification levels.

8-310. Interconnection Memorandum of Agreement (MOA) or Interconnection Agreement.

a. The Department CIO shall provide the policy and standards to assist the components in the preparation of the MOA.

b. A MOA is required for the interconnection of classified computer systems that fall within the purview of organizations outside the DOJ or separate accrediting authorities within the DOJ.

c. The MOA shall stipulate all the terms and conditions of the security arrangements that will govern the operation of the interconnected network. Each MOA must be an attachment to the classified system Certification and Accreditation plan when it is submitted for review and approval.

d. The MOA must provide for the immediate notification of all parties to the MOA any time changes to any IT system affect the security of the system or stipulations of the MOA.

8-311. Wireless. Wireless devices that store, process, and/or transmit classified information shall be handled with the same care that applies to information at the highest classification that the system is certified to process.

a. Only assured channels employing NSA approved, Type-1 end-to-end encryption shall be used to transmit classified information.

b. Under no circumstances shall wireless technologies/devices be used for storing, processing, and/or transmitting classified information without written consent of the DSO.

8-312. Boundary Protection Devices. Only NSA approved devices shall be specified for use in security configurations bridging and protecting networks at various classifications and shall be approved by the Department CIO.

Chapter 9
Communications Security

9-100. General.

a. DOJ 2600.2C, DOJ Security Programs and Responsibilities, establishes the six DOJ Security Programs. The Security Programs apply uniform, consistent and cost effective policies and procedures for the Personnel Security, Document Security, Physical Security, Emergency Planning, Communications Security (COMSEC) and Information Technology Security.

b. Communications Security (COMSEC) is defined as actions taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and the measures to ensure the authenticity of such telecommunications. (NOTE: COMSEC also includes cryptographic-security, emission security, transmission security and physical security of COMSEC material as well as COMSEC information itself.)

c. COMSEC material is that material used to protect U.S. Government transmissions, communications used in the processing of classified or sensitive unclassified information, related to national security, from (access by) unauthorized persons and that material used to ensure the authenticity of such communication.

d. The protection of vital and sensitive information moving over/through government communications systems is crucial to the effective conduct of the government. To this end, a system has been established to distribute, control and safeguard COMSEC material is known as the COMSEC Material Control System (CMCS).

e. Detailed guidance for all DOJ personnel who come in contact with COMSEC material is located in the DOJ COMSEC Manual.

9-101. Responsibilities.

a. The DSO is responsible for development, supervision, and administration of the COMSEC program within the DOJ; promulgation of Department-wide policies and procedures; providing guidance and assistance to DOJ components and organizations; and ensuring compliance with COMSEC policies and procedures.

b. The DSO must ensure the National Security Agency (NSA) approved COMSEC Material Control System (CMCS) is being maintained in accounting for COMSEC material within the DOJ purview.

c. The DSO may appoint a DOJ COMSEC Central Office of Records (COR) Manager. The DOJ COMSEC COR Manager shall be responsible for specifying control criteria for all COMSEC material held within the DOJ and provide assistance to component COMSEC Account Managers. The DOJ COMSEC COR Manager is to assist COMSEC Account Managers in the acquisition, control and disposition of COMSEC material. The functional responsibilities of the COR are delineated in the DOJ COMSEC Manual.

d. The DSO must ensure the Department COR continues to maintain administrative oversight on all facets of the component COMSEC Accounts.

e. DOJ components with a designated COMSEC COR that report directly to the NSA National Office of Records, shall establish a COMSEC program compliant with all NSA, CNSS and Department policy, guidance, and doctrine related to COMSEC.

f. All COMSEC CORs are accountable to, as well as subject to evaluation by the DSO.

g. The DSO must establish procedures to ensure COMSEC Account Managers are properly appointed and trained, and their clearances are verified.

h. The DSO shall establish policies and methods for the conduct of initial risk assessments at all sites where COMSEC material is present, including CCI equipment. Security Program Managers (SPMs) will maintain an official file of all risk assessments, and control measures implemented to minimize risk; for review and update as changes occur and to ensure follow-on risk assessments are conducted periodically.

i. The component SPMs, in which a COMSEC Account and COMSEC Account Manager is established, are responsible for ensuring the effective implementation of COMSEC policies and procedures described in the DOJ COMSEC Manual.

j. The COMSEC Account Manager is responsible for the control of all COMSEC material held within the component they service. This responsibility is delegated to individuals by name through appointment of COMSEC Account Manager and Alternate(s) by the DOJ COMSEC COR Manager. The nominee name is submitted to the DOJ COMSEC COR Manager by the Component SPM.

9-102. Requirements for Security Clearances and Restrictions on Access to COMSEC Material

a. Security Clearance. The administrative process based on the DOJ Personnel Security Regulation, must be followed. This clearance plus a need-to-know is the basis for granting access. Access to classified COMSEC material requires a security clearance equal to or higher than the classification of the COMSEC material involved. Access

to unclassified COMSEC material does not require a security clearance. Revocation of a security clearance revokes access.

b. Access or Need-to-Know. Access to classified COMSEC material must be restricted to properly cleared individuals whose official duties require access to COMSEC material. The fact that an individual has a security clearance and/or holds a certain rank or position, does not, in itself, entitle an individual access to COMSEC material.

9-103. Safeguarding Equipment and Keying Material

a. Physical Security. It is the policy of DOJ that COMSEC material, keying material marked CRYPTO, CCI material and equipment both keyed and un-keyed must be given special attention to ensure that it is afforded the appropriate security based on type and classification. Custodian personnel must be briefed by the COMSEC Manager on the proper handling of COMSEC material.

b. Storage Requirement. It is the policy of DOJ to require COMSEC material that is not under the personal control or observation of an appropriately cleared person to be guarded or stored in a GSA-approved security container, vault, modular vault or secure room with an electronic combination lock. Security forms (e.g., SF-700, SF-701, and SF-702) will be utilized to document proper security of COMSEC materials.

c. Two Person Integrity Requirement. For keys, circuits, and terminal equipment cleared for Top Secret, the Two-Person Integrity (TPI) will be strictly complied with.

d. Destruction. Once COMSEC material is issued to a user, they are responsible for the complete destruction of all superseded COMSEC material held. Users must submit destruction reports to the COMSEC Account Manager. Destruction will be performed by a minimum of two properly cleared individuals.

e. Loss of COMSEC material. In the event of loss of any COMSEC material, prompt action must be undertaken utilizing the procedures outlined in the DOJ COMSEC Manual. If the COMSEC Material cannot be located within a reasonable time, not to exceed 24 hours, the COMSEC Account Manager must be notified utilizing the procedures found in the DOJ COMSEC Manual.

9-104. Audits. The COMSEC Account is subject to an audit at least once every 24 months or on an event driven basis to ensure safeguards are adequate for the protection of COMSEC material. All COMSEC material on the COMSEC Account inventory is subject to a 100% review during the audit. The audit will be announced.

9-105. COMSEC Incident Reporting. It is the policy of DOJ that COMSEC incident reports are made to the COMSEC Account Manager. The manager will assess the reported circumstances and pass the assessment to the DOJ COR Manager who will report; as required, to the National COMSEC Incident Reporting and Evaluation System (NCIRES) and the applicable Controlling Authority.

9-106. Emergency Action Plan (EAP). Managers/Users of COMSEC material and the Component Security Program Manager shall ensure a detailed EAP for all classified material is prepared and updated periodically. All personnel will thoroughly familiarize themselves with the provisions of the EAP. All users are responsible for preparing their own EAP to fit the needs of their component. Emergency destruction plans for COMSEC material is required during natural disasters and terrorist threats. All users outside of the continental United States must maintain an emergency destruction plan.

Chapter 10
Release of Classified Information to Contractors

Section 1.
Classified Contracts

10-100. General. The "National Industrial Security Program" (NISP) was established by Executive Order 12829, as amended, to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government. Under the NISP, contractors are mandated to protect all classified information to which they have been given access or custody by U.S. Government Executive Branch Departments or Agencies. The DOJ participates in the NISP to ensure that any classified information released to or accessed by industry, in connection with DOJ contracts, grants, or related activities, is properly safeguarded in a cost-effective manner.

a. Security Programs Managers must be briefed by the Security and Emergency Planning Staff on their responsibility to ensure implementation of and compliance with the NISP requirements in this chapter.

10-101. Contractor Eligibility for Access to Classified Information. The Office of Personnel Management (OPM), is responsible for conducting the background investigations required for contractor employee access determinations. The Defense Security Service (DSS) is responsible for administering the personnel access authorizations, conducting the inspections required for contractor facility security clearances (FCL), and maintaining the facility clearance records under the NISP.

a. Self-Employed Consultants. Individuals under contract to provide professional or technical assistance to a component in a capacity requiring access to classified information shall be processed for a personnel security clearance (PCL) by the component in accordance with established Department procedures. In this instance a DD Form 254 "Contract Security Classification Specification" is not required; however, components are to ensure that a valid contract containing appropriate security requirements and a Statement of Work are in place. See Annex D for security requirements for classified contracts.

b. Service Contracts. Requests to clear contractors solely to avoid implementing basic security procedures that would otherwise preclude access to classified information, for example, escort by an authorized person in combination with appropriate area sanitization, is not justification for a facility security clearance. In instances where a contractor is required to perform service-oriented tasks and due to the nature of the classified material involved, an area cannot be adequately sanitized to preclude access to classified information even with appropriate escort, components must provide a clear explanation of the rationale for the granting of an FCL by the DSS.

10-102. Foreign Ownership, Control or Influence. U.S. contractors determined to be under foreign ownership, control, or influence (FOCI) are ineligible for an FCL until security measures have been put in place to negate or mitigate FOCI. In instances where a contractor has been determined to be under FOCI, the primary consideration shall be the safeguarding of classified information.

a. FOCI Mitigation. Methods that can be applied to negate or mitigate the risk of foreign ownership or control include board resolution, voting trust agreement and proxy agreement, Special Security Agreement (SSA) and Security Control Agreement. The SSA is an arrangement based upon an assessment of the FOCI factors, that imposes various industrial security export control measures within an institutionalized set of contractor practices and procedures.

b. National Interest Determination. The requirement for a National Interest Determination (NID) applies to new contracts, including pre-contract activities in which access to proscribed information (Top Secret; Communications Security (COMSEC), except classified keys used for data transfer; Restricted Data; Special Access Programs; or Sensitive Compartmented Information) is required, and to existing contracts when contractors are acquired by foreign interests and an SSA is the proposed FOCI mitigation method. A contractor is not eligible for access to proscribed information until the Department completes a National Interest Determination certifying that release of proscribed information to the contractor is consistent with the national security interests of the United States.

(1) When access to proscribed information is required to complete pre-contract award actions or to perform on a new contract, the component shall determine if release of the proscribed information is consistent with national security interests. For contractors with existing contracts that require access to proscribed information, have been or are in the process of being acquired by foreign interest and have proposed an SSA to mitigate foreign ownership, the DSS will notify the OISSO, which will then notify the component of the requirement for a NID.

(2) The preparation of a NID and advisement to the DSS of the intention to provide a NID is the responsibility of the component. The Office of Information Safeguards and Security Oversight (OISSO) will assist components with the NID process when necessary.

(3) NIDs can be program, project or contract specific. A separate NID is not required for each contract under a program or project. The NID decision shall be made at the component Executive Office level.

The NID shall render a determination by the component that release of proscribed information to the contractor shall not harm the national security interests of the United States and must include the following information:

(a) Name and address of Contractor;
(b) Commercial and Government Entity (CAGE) code;
(c) Contract number, program or project name;
(d) The specific category of proscribed information being authorized for release;
(e) Component Point of Contact and telephone number;
(f) The following statement, “Release of the proscribed information to the company will not harm the national security interests of the United States;”
(g) The results of the coordination with national authorities on the release of proscribed information under their jurisdiction (National Security Agency (NSA), Office of the Director of National Intelligence (ODNI) Department of Energy (DoE), etc.), if any; and
(h) The signature of an Executive Office Level individual at the component.

(4) When no interagency coordination is required because the Department owns or controls all of the proscribed information in question, the component shall provide a final documented decision to the OISSO for forwarding to the DSS, FOCI Branch with a copy to the contractor, within 30 days of the date of the request for the NID.

(5) If the proscribed information is under the classification or control jurisdiction of another agency, the component shall advise that agency of such, for example, NSA for COMSEC; ODNI for Sensitive Compartmented Information, DOE for Restricted Data. These agencies must be consulted for a determination that release to the contractor of an entire category of proscribed information under their control will not harm the national security. Written notice must be provided by the component to that agency that its written concurrence is required. Such notice shall be provided within 30 days of being informed by the DSS of the requirement for a NID. Components shall forward a final documented decision to the OISSO for forwarding to the DSS, with a copy to the contractor, within 60 days of the date of the request of the NID.

(6) NIDs shall be coordinated by the component with both the OISSO and the DSS, FOCI Branch located at 1340 Braddock Place, Alexandria, Virginia 22314. The OISSO will then forward the completed NID and signed DD Form 254 to DSS Headquarters with a copy to the appropriate DSS field office.

10-103. Generating a Classified Contract or Contract Solicitation. Participation in the NISP allows DOJ to use the DSS to conduct inspections for contractor facility, administer personnel clearances and to monitor the contractor's compliance with safeguarding requirements. There is no charge for these services. In order to activate DSS services and obligate the contractor to the provisions of the National Industrial Security Program Operating Manual (NISPOM), a DD Form 254 "Contract Security Classification Specification" must be included in all classified contracts and contract solicitations.

10-104. Initiating a DD Form 254. Components that have established a requirement to initiate a contract or contract solicitation under the NISP should use the following procedures.

a. The requesting component shall ensure the contractor requires access to classified information to perform the contract specifications. The NISP is for classified National Security Information contracts only.

b. The component shall provide the OISSO with the highest security clearance level and storage requirements of the contract. For contract DD Form 254s, the name, address, and telephone number of the prospective contractor, (solicitation DD Form 254s will not identify a contractor), a copy of a valid Statement of Work, plus appropriate security clauses also will be provided. This information may be provided via FAX on 202-616-1416, via JCON e-mail to the OISSO or normal mail channels.

c. The OISSO shall determine the contractor clearance status and initiate action for the proper FCL if it is not in place. The OISSO will notify the requesting component of the clearance status of the contractor within five working days.

d. Components shall prepare the DD Form 254. Instructions for the completion of the DD Form 254 are included with the form. The OISSO will assist the components in the completion of the DD Form 254 when necessary. When complete, the DD Form 254 must be forwarded to the OISSO for review and signature by the DSO.

e. The OISSO will provide a copy of the signed DD Form 254 to the component for inclusion in the contract or contract solicitation. The OISSO will send the original DD Form 254s to the DSS which will arrange for OPM to conduct the required background investigations. The DSS will then conduct security oversight functions in coordination with the Contractor's Facility Security Officer and the requesting component. DD Form 254s approved solely for contract solicitation will not be forwarded to the DSS.

f. In some instances it may be necessary to include classified information in DD Form 254s and facility clearance requests. In these instances the documentation must be transmitted in a manner approved for classified information.

Section 2.
Classified Contractor Visits

10-200. General. A visit will be considered a classified visit when it requires, or is anticipated to require that the visiting contractor will receive or have access to classified information.

10-201. Approval of Classified Visits.

a. All classified visits to components by contractors require advance notification to, and approval of, the component hosting the visit.

b. A visit request shall be in writing and may be submitted either by mail, facsimile, teletype, or courier in sufficient time to allow the component to approve or disapprove the requested visit. In urgent cases, a visit request may be made by telephone, provided written confirmation follows.

c. The component having security cognizance has final approval authority for the proposed visit. A requester can assume approval of a visit only if sufficient advance notice of the visit was provided. If a proposed visit is disapproved, the requester must be promptly notified.

d. The number of classified visits shall be held to a minimum. The component must determine that the visit is necessary and requires access to classified information in order to approve a classified visit.

10-202. The Visit Authorization.

a. The visit authorization letter (VAL) provides advance notification of the intent to visit and certifies the clearance level and need to know of the visitor.

b. A request shall contain as a minimum, the following information:

(1) Contractor's name, address, and telephone number, assigned Commercial and Government Entity (CAGE) Code, if applicable, and certification of the level of the facility security;

(2) Name, job title or position, date and place of birth, and citizenship of the employee intending to visit;

(3) Certification of the proposed visitor's personnel clearance and any special access authorizations required for the visit;

(4) Name and title of person(s) to be visited;

(5) Purpose and justification for the visit in sufficient detail to allow for a determination of the necessity of the visit. Include a contract number, project or program number, or name to assist the recipient in making this determination; (do not use nicknames, abbreviations, or acronyms);

(6) Date or period during which the VAL is valid, not to exceed 12 months.

10-203. Precautions During Visits.

a. Visitors should not be permitted to take notes, make records of classified discussions, or take photographs in areas where classified information might be recorded, unless given permission by the host DOJ component or office, or as otherwise specified in a classified contract.

b. Classified material received during the visit shall be safeguarded as required by the NISPOM.

c. Access to classified information, higher than the level of the visitor's clearance certified in the visit request, shall not be granted. Access shall not be granted if the level of classified information exceeds the level required by a contract or specific purpose identified in the VAL.

10-204. Rosters. Rosters of contractor employees may be used to establish visit requests and approval authorizations as required by this Section, provided:

a. The roster or cover letter furnishes the information required by 10-202 of this Section;

b. The roster is limited to contractor employees who have authorized access to particular levels of classified information and occupy positions that require classified visits;

c. The procedures in effect are adequate to notify the component honoring such a roster of changes in employees' status that will affect the visit authorization;

d. The use of such procedures is acceptable to the component hosting the visit; and

e. The rosters are maintained in a current status at all times.

Chapter 11
Special Access Programs

Section 1.
Introduction

11-100. General.

a. Special Access Programs (SAPs) are programs established for a specific class of classified information that imposes safeguarding requirements that exceed those normally required for information at the same classification level.

b. 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 SAP. For SAPs 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 (DNI).

c. Executive Order 13526 requires that the number of SAPs be kept at an absolute minimum and shall be established 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.

d. The Attorney General may enhance the safeguarding requirements in this manual for information in SAPs and shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

e. The Attorney General is responsible for ensuring 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.

11-101. Requirements and Limitations of SAPs.

a. SAPs 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.

b. The Attorney General shall establish and maintain a system of accounting for SAPs consistent with directives issued pursuant to EO 13526.

c. Special access programs shall be subject to the oversight program established under section 5.4(d) of E.O. 13526. The Director of the Information Security Oversight Office (ISOO) 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 ISOO under E.O. 13526. The Attorney General may limit access to a SAP to the Director of the ISOO and no more than one other employee of the ISOO or, for SAPs that are extraordinarily sensitive and vulnerable, to the Director only.

d. The Attorney General shall brief the National Security Advisor, or a designee, on any or all of the DOJ's SAPs upon request.

11-102. Establishing a SAP.

a. Any time a component initiate's involvement in a SAP the Department Security Officer (DSO) must be notified.

b. The establishment of SAPs within the DOJ is the responsibility of the Attorney General. Components may submit a written request with justification for the establishment of a SAP to the DSO for appropriate action when:

(1.) A component is the sponsor of a classified program requiring special safeguarding measures by statute; or

(2.) A component originates specific information it believes the vulnerability of, or threat to, is exceptional and 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.

c. The operation of an unauthorized SAP may result in the suspension/revocation by the DSO of the DOJ national or special security access clearances of DOJ employees who are not in compliance with paragraph 11-100.b. above.

11.103. Annual review and Accounting for SAPs.

a. The Attorney General or the Deputy Attorney General shall review each SAP annually to determine whether it continues to meet the requirements of E.O. 13526.

b. The DSO shall annually review and account for DOJ SAPs to ensure that the enhanced controls are based on an assessment of the value, critical nature and vulnerability of the information in accordance with E.O. 13526.

11-104. Sensitive Compartmented Information (SCI). SCI is a term referring to SAPs established by the

DNI pertaining to information concerning or derived from intelligence sources, methods, or analytical processes and requiring handling exclusively within formal access control systems. SCI is also referred to as "codeword" information. The sensitivity of this information requires that it be protected in a much more controlled environment than other classified information. Therefore, the DNI has established special policies and procedures for the protection of SCI.

Section 2.
Administration of the SCI Program

11-200. General. The remainder of this chapter provides general guidance to DOJ component SPMs regarding the storage, use, discussion and/or processing of SCI. The DSO shall provide detailed information and guidance to component SPMs, as appropriate to their need, to participate in the SCI program.

11-201. Responsibilities.

a. The Federal Bureau of Investigation (FBI) and Drug Enforcement Administration (DEA), as members of the intelligence community, shall independently administer their SCI program consistent with DNI directives and subject to security oversight by the DSO. The DSO shall administer all other aspects of the DOJ's SCI program.

b. The DSO has delegated the responsibility for the daily operation of the SCI program to the Assistant Director, Office of Information Safeguards and Security Oversight (OISSO), who shall appoint a member of the DOJ Special Security Center (SSC) to serve as the DOJ Special Security Officer (SSO). All routine matters pertaining to the operations of the SCI program should be addressed to the SSO located in the Special Security Center, Room 6222, Main Justice Building, 950 Pennsylvania Avenue, NW, Washington, D.C. 20530. Phone: (202) 514-3738. Fax: (202) 616-1416.

11-202. Basic SCI Controls. The requirements outlined below must be followed when handling SCI.

a. SCI material must only be disseminated on a need-to-know basis to individuals who hold the proper access (i.e., SI, TK, G, etc.) for the program. If it is not known if an individual within the component is cleared for a specific SCI access, the Security Programs Manager (SPM) should be contacted. If the individual is in another component, contact the SSC on (202) 514-3738 to verify the individual's SCI access.

b. SCI information may only be discussed, processed and/or stored within a Sensitive Compartmented Information Facility (SCIF). The component SPM or DSO can advise component employees regarding the location of accredited SCIFs. The DSO can provide information on SCIFs located in other components or facilities.

c. SCI material must not be sent to a building that does not have a SCIF or to someone who does not have access to a SCIF. When necessary, arrangements can be made to have the SCI material held at the SSC, Room 6222 MAIN, and the intended recipient should be advised that it can be read, processed and stored there.

d. SCI materials sent between SCIFs must be hand-carried by individuals that are properly briefed on courier procedures, possess a courier card at the appropriate level, and are cleared for the material being couriered. Materials carried within a building should be in a sealed opaque envelope that is properly addressed, and materials transported between buildings must be double-wrapped, in the same manner required for National Security Information, see Chapter 6.

e. All SCI materials must be properly marked and have appropriate cover sheets attached.

f. SCI can be processed only on a computer that has been specifically accredited for that purpose. The computer must be located in an accredited SCIF.

g. Personnel who hold access to SCI material must receive periodic refresher briefings on the procedures for handling SCI materials. The SSC can provide these briefings at the request of the SPMs.

h. Any loss, compromise or suspected compromise of SCI materials must be immediately reported to the DSO.

Section 3.
SCI Access Authorizations

11-300. SCI Access Process.

a. Request for access to SCI shall be submitted in writing to the DSO. The request shall specify the access required and justification for the access request. If the DSO is not the servicing personnel security office for the requestor, the SPM must submit the personnel security records for the individual along with the request to the DSO.

b. In order for an individual to be considered for access to SCI, they must have a Top Secret access authorization based on a current background investigation. If an appropriate current background investigation has not been completed the servicing personnel security office shall initiate the appropriate background investigation.

c. The DSO shall adjudicate the background investigation in accordance with guidelines established by the DNI and grant SCI access accordingly. The DSO shall consult with the DNI concerning any questionable background information that might be grounds for a denial of access. Decisions to deny access authorizations to SCI will be made by the DNI or DNI representative.

d. Interim Access. In exceptional cases, the DSO may grant temporary access to SCI where official functions must be performed prior to the completion of the appropriate background investigation. The temporary access will be valid until completion and adjudication of the investigation

and will be reviewed after 180 days. However, the DSO may suspend the interim access at any time based on unfavorable information identified in the course of the investigation. Certifications to other agencies must disclose the temporary access and other agencies do not have to accept the certification. Temporary access may be granted after the following minimum requirements have been met.

(1) For individuals who are not the subject of a current, favorably adjudicated investigation of any kind: completion and review of an SF 86, including any applicable supporting documentation, favorable review of a credit check, submission of an expedited Single Scope Background Investigation (SSBI), and completion and favorable review of relevant criminal history and investigative records of the FBI and information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII). A National Crimes Information Center (NCIC) check may be used pending completion of the FBI name and fingerprint checks.

(2) For individuals who are the subject of a current and favorable background investigation not meeting the investigative standards for access at the SCI level; completion and review of an SF 86, including any applicable supporting documentation, favorable review of a credit check, and submission of an expedited SSBI.

(3) All requests for temporary access to SCI will require a written request from the Head of the Component or designee (designation must be in writing and a copy must be furnished to the office granting the temporary access) stating the compelling need for the temporary access.

e. Prior to being afforded access to SCI, persons approved for SCI access, shall be briefed by the SSC. The briefing shall consist of non-SCI-revealing information of a general nature on procedures for protecting the SCI to which they will be exposed, advised of their obligations both to protect that information and to report matters of security concern, and allowed to express any reservations concerning the required Nondisclosure Agreement or access to SCI. After the person has signed the required Nondisclosure Agreement, they will be further indoctrinated into the specific SCI programs for which they have been approved access.

f. As a condition of access to SCI, individuals must sign a DNI -authorized Nondisclosure Agreement (NdA) (Form 4414), which includes a provision for pre-publication review. The NdA establishes explicit obligations on both the government and the individual for the protection of SCI. Failure to sign an NdA is cause for denial or revocation of existing SCI access.

g. Employees with access to SCI will be subject to reinvestigations every 5 years and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access.

h. An additional requirement for access to SCI is that individuals must sign a "Consent for Warrantless Searches of Department of Justice Workplaces." This was approved by the Attorney General in December 2001 and applies to all DOJ employees requiring access to SCI and for employees with access to classified information designated by the Component Head.

11-301. Reporting Foreign Travel. Persons currently approved for SCI access who plan unofficial travel to or through, or who are being assigned to duty in, foreign countries must provide through the SPM to the DSO advance written notice of the travel. Form DOJ-504, "Notification of Foreign Travel," is recommended for making this notification. When determined as necessary by the DSO, the person must receive an appropriate defensive security briefing prior to the official assignment or unofficial travel.

11-302. Pre-publication Review. Persons who are currently approved for SCI access or who have held SCI access approval must submit to the National Security Division, which is the appropriate approving authority, all articles and publications for review if there is any possibility that the publication may contain SCI or information acquired as a result of SCI access.

11-303. Debriefing. When an SPM or supervisor has determined that access to SCI or specific SCI compartments is no longer required, security debriefing instructions and guidelines will be provided to that employee. At a minimum these shall include:

a. A requirement that the individual read appropriate sections of Titles 18 and 50, United States Code, and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

b. The continuing obligation, under the pre-publication review and other provisions of the NdA for SCI, never to divulge, publish, or reveal by writing, word, conduct, or otherwise, to any unauthorized persons any SCI, without the written consent of appropriate DOJ officials.

c. An acknowledgement that the individual will report without delay to the FBI and/or the DSO, any attempt by an unauthorized person to solicit National Security Information.

d. A declaration that the individual no longer possesses any documents or material containing SCI.

e. A reminder of the risks associated with foreign travel and foreign association.

Section 4.
Sensitive Compartmented Information Facility (SCIF)

11-400. General. All SCI must be stored, used, discussed, and/or processed within accredited SCIFs. SCIF's and all systems processing SCI information must be accredited by an Organization that is a member of the Intelligence Community. All non-intelligence community organizations must have their SCI facilities and systems accredited by the Central Intelligence Agency (CIA) through the DSO. The FBI and DEA are the only DOJ components that are members of the Intelligence Community per EO 12333. Components shall request the establishment of a SCIF only when there are clear operational requirements and when existing SCIFs are not adequate to support the requirements.

11-401. Procedures for Establishing SCIFS.

a. When it is determined that a SCIF is necessary for an SCI program, the component SPM will contact the DSO and arrange for a survey of the proposed SCIF. The DSO will provide security specification for construction of the SCIF in accordance with current DNI standards, taking into consideration environmental factors and the intended use of the SCIF.

b. A SCIF Control Officer (SCO) and Alternate Control Officer(s) (ACOs) will be designated in writing by the component SPM. The SCO shall be responsible for implementing the safeguards required for the SCIF and the Standard Operating Procedures (SOP).

c. The SPM shall ensure the SCIF is constructed in accordance with the security specification provided by the DSO. Upon completion of construction, the DSO shall conduct an inspection of the facility to ensure it meets DNI standards.

d. The DSO shall prepare the required fixed facility checklist and Standard Operating Procedures (SOP) with the assistance of the component SPM. The SCO shall ensure the SOP is fully implemented.

e. Upon final inspection of the SCIF by the DSO and a final review and approval of the required SCIF documentation and procedures, the SCIF will be inspected by the Central Intelligence Agency (CIA) for final accreditation. The FBI and DEA are members of the Intelligence community and have final Accreditation authority for their individual SCIF's.

f. The SCO must obtain DSO approval prior to any changes in the SCIF construction or the operating procedures.

Section 5.
SCI Computer Systems

11-500. General. Information Technology (IT) systems used to process, store or handle SCI must be operated so that the information is protected against unauthorized disclosure, modification, access, use, destruction, or delay in service.

a. All IT systems that process, store or handle SCI must be approved by the DSO and accredited by the same organization that accredited the SCIF it will located in prior to their operation.

b. All IT systems processing SCI must follow the requirements delineated in Intelligence Community Directive (ICD) 503.

c. Due to the complexity of the requirements for IT systems processing SCI, all IT systems must be approved through the DSO. As such, the DSO is the ONLY entity authorized to acquire approval and accreditation of IT systems for processing SCI through the agency that approves the SCI Facility.

d. SCI systems will not be placed in operation until authorized in writing by the DSO.

11-501. Procedures for requesting authorization for SCI IT Systems. When the need to process SCI information becomes apparent, the SPM or designee should contact the DSO. The DSO will provide support in defining your organization's needs and the requirements necessary to meet those needs. The DSO shall provide support to the SPM in developing security related documentation for the approval process.

Section 6.
Clearance Certifications

11-600. General. DOJ employees holding SCI access that plan to attend meetings, document reviews, conferences, or other similar events at other organizations where the discussion of SCI will occur may be required to have their SCI access certified to the agency or organization sponsoring the event.

11-601. Procedures for Requesting the Passing of a Clearance.

a. Requests for access certification may be accomplished through the SPM by facsimile, or e-mail to SSC@usdoj.gov, and should be forwarded to the SSC as soon as the date(s) of the event is known.

b. The request for SCI access certification shall contain the following information

(1.) Full name;

(2.) Social Security Number;

(3.) Department Component;

(4.) SCI Access compartments to be certified;

(5.) Name of the organization where the event will take place, including an office identifier, if any;

(6.) Organization point of contact;

(7.) Point of contact telephone number;

(8.) Dates of the event;

(9.) Purpose of the event; and

(10.) The effective date(s) or period (up to one year) for the certification.

Chapter 12
Accounting for Cost

Section 1.
Introduction

12-100. General.

a. The estimated costs associated with the classification and safeguarding of classified information must be reported annually by the DOJ to the Information Security Oversight Office (ISOO) in accordance with Executive Order 13526. The ISOO provides these estimated costs annually to the President.

b. The cost estimates reported shall distinguish classified information costs from other security costs. Security cost which would be incurred independent of classified information activities, such as security guards and security alarms to protect life and property shall not be reported. Counterintelligence resources shall not be included in the data collection.

c. If 51% or more of a resource is devoted to a classification related activity, it should be included in the estimate. Only those cost estimates associated with classification-related activities should be reported.

12-101. Responsibilities.

a. The Department Security Officer (DSO) shall work closely with the Security Programs Manager (SPM) and the DOJ Comptroller to ensure that the best estimates are collected for each of the cost categories identified below.

b. Each component shall provide the cost data for the previous fiscal year to the DSO by February 1, of each year.

c. The DSO will review the data for consistency and compile the data for the DOJ report.

Section 2.
Cost Categories

12-200. General.

a. Estimated costs for the protection of classified information must be reported under one of the categories listed below. In some instances, the DSO already may have the data for a particular category and the SPM will be advised to disregard collecting that data.

b. The cost incurred within each category need not be itemized. A single aggregate cost for each category should be submitted. Components are to report actual dollar amounts instead of thousands.

c. In instances where there is a significant difference between the total figures reported for each fiscal year, components must provide an explanation in narrative form for inclusion in the Department's report to the ISOO.

12-201. Personnel Security.

a. Cost estimates for background investigations shall only include the difference between the cost for investigations required for access to classified information and the investigation normally required by the DOJ for an individual serving in a similar position.

b. Report only those personnel security cost estimates associated with access to classified information.

(1) Clearance Program. Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

(2) Initial Investigations. Completing and reviewing a Personnel Security Questionnaire, initial screening, filing data in the Central Personnel Database, forwarding to the appropriate investigative authority, and the investigation itself.

(3) National Agency Check. Include only when used for the basis of granting a clearance.

(4) Adjudication. Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

(5) Re-investigations. Periodic recurring investigations of Government and contractor personnel.

(6) Polygraph. Substantive examinations in the security screening process.

12-202. Physical Security. That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign. Report only those physical security cost estimates associated with classification related activities.

a. Physical Security Equipment. Any item, device, or system that is used primarily for the protection of classified information and installations.

b. Protective Forces. All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and

supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

c. Intrusion Detection and Assessment. Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

d. Barrier/Controls. Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

e. Vital Components and Tamper-Safe Monitoring. Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

f. Access Control/Badging. Personnel and hardware such as badging systems, card-readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

g. Visitor Control. Personnel and activities associated with processing visitors for access to facilities holding classified information.

12-203. Information Security. Report only those Information Security cost estimates associated with classification related activities.

a. Classification Management. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

b. Declassification. Declassification encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive order or statute.

c. Information Systems Security for Classified Information. Security of these systems involves the protection of information systems against unauthorized access to or modifications of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

(1) Information Systems Security Engineering. The process that captures and refines information protection requirements and ensures their integration into information technology acquisition processes through purposeful security design or configuration.

(2) Information Systems Security Equipment Modification. Modification of any fielded hardware, firmware, software, or portion thereof, under National Security Agency configuration control There are three classes of modifications: mandatory to include human safety; operational/special mission modifications; and repair actions. These classes apply to elements, subassemblies, equipment, systems, and software packages performing functions such as key generation, key distribution, message encryption, decryption, authentication, or those mechanisms necessary to satisfy security policy, labeling, identification, or accountability.

(3) TEMPEST. The investigation, study and control of compromising emanations from information systems equipment.

(4) Communications Security (COMSEC). Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

d. Miscellaneous.

(1) Operations Security (OPSEC). Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis vulnerabilities, assessment of risks, and application of appropriate countermeasures.

(2) Technical Surveillance Countermeasures (TSCM). Personnel and operating expenses associated with the development, training and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches and telephone system searches.

12-204. Professional, Education, Training and Awareness. The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information. Report only those security education training and awareness cost estimates associated with the security of classified information.

12-205. Security Management, Oversight and Planning. The development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities and respond to management requests related to classified information. Report only those security management, oversight, and planning cost estimates associated with managing classified information.

a. Research, Test, and Evaluation. The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

b. Surveys, Reviews, Accreditation, and Assessments. Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

c. Special Access Programs. Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs in this section that have been reported under the other primary categories.

d. Security and Investigative Matters. The investigation of security incidents, infractions, and violations.

e. Industrial Security (Non-Contractor Costs). Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. These activities may include industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration. Report only those cost estimates associated with component management of the industrial security program.

f. Foreign Ownership, Control, or Influence (FOCI). The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

12-206. Unique Items. Items that are not reported in one of the primary categories, but represent significant costs must be reported as a unique cost. Unique items must include a narrative on why it should be included and how the figures were developed. Report only those cost estimates associated with activities pertaining to the security of classified information.

Chapter 13
Self-Inspection Review Program

Section 1.
Introduction

13-100. General. This portion of the manual sets standards for establishing and maintaining an ongoing department self-inspection review program, which shall include regular reviews and assessments of representative samples of the DOJ's original and derivative classification actions. The DOJ's security review program includes the review and evaluation of individual component activities and the DOJ as a whole with respect to the implementation of the classified information programs established under Executive Order 13526 its implementing directive.

13-101. Responsibilities. The senior agency official is responsible for directing and administering the DOJ's security review program. The senior agency official has designated the Department Security Officer (DSO) to implement the DOJ 's security review program. To supplement the DSO inspection program, each component with significant involvement with classified national security information shall establish an internal security review program of its own that meets the requirements of this chapter. The security review 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 DOJ components and the DOJ as a whole, in order to enable the senior agency official to fulfill his or her responsibility to oversee the DOJ's program under section 5.4(d) of the Order.

13-102. Approach. The DSO shall determine the means and methods for the conduct of self-inspections:

a. Self-inspections shall evaluate the adherence to the principles and requirements of the Order and its implementing directive and the effectiveness of DOJ's programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training and management and oversight;
b. Regular reviews of representative samples of the DOJ's original and derivative classification actions shall encompass all agency components that generate or handle 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 DOJ's classified product. DOJ personnel who are assigned to conduct reviews of DOJ's original and derivative classification actions shall be knowledgeable of the classification and marking requirements of the Order and its implementing directive, and have access to pertinent security classification guides. In accordance with section 5.4(d)(4) of the Order, the DSO shall authorize appropriate agency officials to correct misclassification actions; and
c. Self-inspections shall include a review of relevant security directives and instructions, as well as interviews with producers and users of classified information.

13-103. Frequency.

a. Self-inspections shall be regular, ongoing, and conducted at least annually with the DSO setting the frequency on the basis of program needs and the degree of classification activities.

b. Components who handle and safeguard classified information must conduct at least one internal security review a year, in addition to reviews conducted by the DSO. Each component shall provide the Security Review Report (SRR) for the previous fiscal year to the DSO by October 15th of each year. Components that generate significant amounts of classified information shall include a representative sample of their original and derivative classification actions.

c. The frequency of DSO security reviews shall be based on program needs and the degree of classified activity.

13-104. Reporting.

a. The DOJ shall document the findings of self-inspections internally.

(1.) Internal. The DSO 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:
  (a.) A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized;
  (b.) 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;
  (c.) 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;
  (d.) Actions that have been taken or are planned to correct identified deficiencies or misclassification actions, and to deter their reoccurrence; and

(e.) Best practices that were identified during self-inspections.

b. All deficiencies identified during a review shall be documented in the SRR. SRRs are due as a matter of course and not just in instances of significant findings.

c. Security incidents identified during a review shall be reported to the DSO pursuant to the security incident reporting requirements outlined in Chapter 1.

Section 2.
Elements of Review

13-200. Coverage. Each component may expand the review according to program and policy needs but must include, as a minimum, all applicable elements covered in this chapter.

13-201. Original Classification.

a. Evaluate Original Classification Authority's (OCA) general understanding of the process of original classification, including the:

(1.) Applicable standards for classification;

(2.) Levels of classification and the damage criterion associated with each; and

(3.) Required classification markings.

b. Determine if delegations of OCA conform with the requirements of Executive Order 13526, including whether:

(1.) Delegations are limited to the minimum required to administer the program;

(2.) Designated OCAs have a demonstrable and continuing need to exercise this authority;

(3.) Delegations are in writing and identify the official by name or position, title; and

(4.) New requests for delegation of classification authority are justified.

c. Assess OCA's familiarity with the duration of classification requirements, including:

(1.) Establish a specific date or event for declassification at the time of original classification based on the duration of the national security sensitivity of the information;

(2.) Determining a date or event that is less than 10 years from the date of original classification which coincides with the lapse of the information's national security sensitivity, and assigning such date or event as the declassification instruction;

(3.) Assigning ordinarily a declassification date that is 10 years from the date of the original classification decision if unable to determine a date or event of less than 10 years; and

(4.) Assigning a declassification date not to exceed 25 years from the date of the original classification decision if unable to determine a date or event of 10 years.

d. Conduct a review of a sample of classified information generated by the inspected activity (or activities) to determine the propriety of classification and the application of proper and full markings.

e. Evaluate the classifiers' knowledge of the preparation and use of Classification and Declassification Guides.

f. Verify observance with the prohibitions on classification and limitations on reclassification.

g. Assess whether the DOJ's classification challenges program is properly implemented.

13-202. Derivative Classification. Assess the general familiarity of individuals who classify derivatively with the:

a. Conditions for derivative classification;

b. Requirement to consult with the originator of the information when questions concerning classification arise;

c. Proper use of classification guides; and

d. Proper and complete application of classification markings to derivatively classified documents.

13-203. Declassification and Downgrading.

a. Verify whether the DOJ has established, to the extent practical, a system of records management to facilitate public release of declassified documents.

b. Evaluate the status of the DOJ declassification program, including the requirement to:

(1.) Comply with the automatic declassification provision regarding historically valuable records over 25 years old;

(2.) Declassify, when possible, historically valuable records prior to accession into the National Archives and Records Administration;

(3.) Provide the Director, National Declassification Center, with adequate and current declassification guides;

(4.) Ascertain that the DOJ's mandatory review program conforms to established requirements; and

13-204. Safeguarding.

a. Assess adherence to the standards contained in this manual.

b. Assess compliance with controls for access to classified information.

c. Evaluate the effectiveness of the component's program in detecting and reporting security violations and preventing recurrences.

d. Assess compliance with the procedures for identifying and reporting unauthorized disclosures of classified information.

e. Evaluate the effectiveness of procedures to ensure that:

(1.) The originating component exercises control over the classified information it generates;

(2.) Holders of classified information do not disclose information originated by another agency without that agency's authorization; and

(3.) Departing or transferred personnel return all classified information in their possession to authorized agency personnel.

f. Ensure all computers used to process classified information are certified and accredited in accordance with Chapter 8 of this manual.

13-205. Security Education and Training. Evaluate the effectiveness of the DOJ's security education and training program in familiarizing appropriate personnel with classification procedures; and determine whether the program meets the standards specified in Chapter 3 of this manual.

13-206. Management and Oversight.

a. Determine whether designated OCAs have received training in original and derivative classification.

b. Verify whether the component's SAP's:

(1.) Adhere to specified criteria in the creation of these programs;

(2.) Are kept to a minimum;

(3.) Provide for the conduct of internal oversight; and

(4.) Include an annual review of each program to determine whether it continues to meet the requirements of Executive Order 13526 and this manual.

c. Assess whether:

(1.) Senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;

(2.) Producers and users of classified information receive ongoing guidance with respect to security responsibilities and requirements;

(3.) Controls to prevent unauthorized access to classified information are effective;

(4.) Contingency plans are in place for safeguarding classified information used in or near hostile areas;

(5.) The performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element to be evaluated in the rating of OCAs, SPMs or security specialists and other employees significantly involved with classified information; and

(6.) A method is in place for collecting information on the costs associated with implementation of national security requirements in accordance with Chapter 12.

d. Verify that all classified information released to industry is covered by a DD Form 254 and subject to the provisions of the National Industrial Security Program.

Chapter 14
Restricted Data and Formerly Restricted Data

Section 1.
Introduction

14-100. General. This chapter establishes Department policy for the classification and declassification of Restricted Data (RD) and Formerly Restricted Data (FRD) pursuant to the Atomic Energy Act of 1954 as promulgated by 10 CFR Part 1045 "Nuclear Classification and Declassification". These policies and procedures apply to any Department of Justice (DOJ) employee and DOJ contractor who has authorized access to RD or FRD or generates information that may be determined to be RD or FRD.

14-101. Definitions.

a. Restricted Data (RD:) Classified information that consists of all data concerning the following, but not including data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act: (1) design, manufacture, or utilization of Atomic Weapons; (2) production of Special Nuclear Material (SNM); or (3) use of SNM in the production of energy.

b. Formerly Restricted Data (FRD): Classified information jointly determined by DOE and the Department of Defense (DoD) to be related primarily to the military utilization of atomic weapons and removed (by transclassification) from the RD category pursuant to section 142(d) of the Atomic Energy Act.

c. Restricted Data Classifier: Individuals who derivatively classify RD or FRD documents. Within the DoD, RD Classifiers may also declassify FRD documents.

d. Special Nuclear Material: Plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which the Secretary of Energy determines to be SNM pursuant to the Atomic Energy Act.

e. Transclassification: Information that has been removed from the RD category by a joint determination of DOE and DoD and placed in the FRD category in accordance with section 142(d) of the Atomic Energy Act.

14-102. Responsibilities. Ensure that RD Classifiers are trained on the proper procedures for classifying, marking, handling, and declassifying RD and FRD documents and all employees with access to RD and FRD information are trained on the authorities required to classify and declassify RD and FRD information and documents and on handling procedures.

a. Attorney General. The Attorney General shall:

(1) Ensure that RD and FRD information, documents, and material are reviewed and processed in accordance with requirements in this chapter.

(2) Ensure that an RD Management Official is appointed to implement these policies and procedures within the DOJ and provides notification to the DOE Director, Office of Classification and Information Control (OCIC) of the appointment.

(3) Ensure that the performance of classification and declassification activities by the RD Management Official is evaluated periodically.

(4) Ensure that the performance of RD Classifiers who classify or declassify significant numbers of RD or FRD documents is evaluated periodically.

b. Department Security Officer. See Chapter 1, "General Provisions and Requirements;" Section 2, "General Requirements;" 1-200a. (1) - (3), "Responsibilities."

c. RD Management Official. The Assistant Director, Office of Information Safeguards and Security Oversight is designated the RD Management Official at the Department of Justice. The RD Management Official shall:

(1) Ensure the implementation of the provisions of 10 CFR Part 1045 within the DOJ.

(2) Serve as the primary point of contact with the DOE Director, OCIC, on RD and FRD classification and declassification issues affecting DOJ employees and DOJ contractors. This individual shall cooperate and provide information as necessary to the DOE OCIC to fulfill responsibilities.

(3) Ensure that individuals within the DOJ who are authorized to derivatively classify RD and FRD documents are designated in writing by position or name as RD Classifiers.

(4) Ensure that classification guides covering RD and FRD information are developed jointly with the DOE for programs with shared responsibility.

(5) Ensure that classification guides that contain RD or FRD topics are coordinated with the DOE OCIC control prior to issuance or when updated.

(6) Ensure that classification guides that contain RD or FRD topics are reviewed at least once every 5 years to ensure consistency with DOE classification policy and revised as necessary.

(7) Ensure that DOJ employees and DOJ contractor personnel who generate RD and FRD documents have access to any nuclear classification guides as needed.

(8) When required, request an exemption from procedural provisions of 10 CFR Part 1045 from the DOE Director, OCIC.

(9) Serve as a member of the standing group of RD Management Officials to address issues concerning implementation of 10 CFR Part 1045.

(10) Determine jointly with DOE if an onsite review within the DOJ by DOE would be mutually beneficial or is necessary to remedy a problem.

d. Head of DOJ contractor. The Head of DOJ contractor shall:

(1) Ensure that employees within the contractor organization who are authorized to derivatively classify RD and FRD documents are designated in writing by position or name as RD Classifiers.

(2) Ensure that RD Classifiers are trained on the proper procedures for classifying, marking, handling, and declassifying RD and FRD documents and all contractor employees with access to RD and FRD information are trained on the authorities required to classify and declassify RD and FRD information and documents and on handling procedures.

(3) Ensure that classification guides covering RD and FRD information are developed jointly with the DOE for programs with shared responsibility.

(4) Ensure that classification guides that contain RD or FRD topics are coordinated with the DOE OCIC prior to issuance or when updated.

(5) Ensure that the classification guides that contain RD or FRD topics are reviewed at least once every 5 years to ensure consistency with DOE classification policy and revised as necessary.

e. RD Classifiers. RD Classifiers shall:

(1) Complete a training program as determined by the RD Management Official. Upon successful completion of the training, the RD Classifier will be designated by the RD Management Official as an RD Classifier for a period of 5 years. After 5 years, the need for such authority shall be reexamined and if still required, the individual shall successfully complete a refresher training session specified by the RD Management Official before being redesignated for additional years.

(2) Classify and declassify RD and FRD documents according to the specifications and requirements cited in this chapter.

(3) Provide classification/declassification assistance and services cited in this chapter.

f. DOJ Personnel/DOJ Contractor Personnel. DOJ personnel and DOJ contractor personnel shall:

(1) Submit any document they originate or possess in an RD or FRD subject area to an RD Classifier for classification review and a determination prior to dissemination.

(2) Submit any document they originate or possess in an RD or FRD subject that is intended for widespread distribution or public release to the DOE OCIC for RD or to the DOE OCIC or appropriate Department of Defense Organization for FRD for classification review and a determination prior to dissemination

Section 2.
Qualifications and Designations

14-200. RD Management Official. Individuals designated by the Attorney General as an RD Management Official must have access to RD and FRD and an in-depth knowledge of RD and FRD classification requirements.

14-201. RD Classifiers. Individuals designated as an RD Classifier by the RD Management Official must have demonstrated competence in the subject area for which the authority will be used and be familiar with classification policy, procedures, and guidance in the area for which the authority will be used. All RD and FRD Classifiers shall be trained in the proper procedures for classifying, marking, handling, and declassifying of such information and documents.

14-202. Requests for RD Classifiers. Components shall limit requests for RD Classifiers to those positions that have a demonstrable and continuing need to exercise this authority. All requests for RD Classifiers shall be submitted in writing to the RD Management Official and include the position and justification for the request. The RD Management Official shall maintain a current listing of positions within the DOJ with authority as RD Classifiers.

Section 3.
Training Requirements

14-300. General.

a. All individuals with access to RD and FRD information shall be trained on the authorities required for classifying, marking, handling, and declassifying RD and FRD information and documents.

b. RD Classifiers shall be trained on the procedures for classifying, marking, handling, and declassifying RD and FRD information and documents.

Section 4.
Classification Guidance

14-400. Developing guidance covering RD or FRD information.

a. Classification guides prepared for programs involving RD or FRD information under the shared responsibility of the DOJ and the DOE must be developed jointly with the DOE OCIC. DOJ components may contact the RD Management Official for assistance with this process.

b. Any classification guide that contains RD or FRD topics shall be coordinated with the DOE OCIC. DOJ components may contact the RD Management Official for assistance with this process.

14-401. Review of Guidance. Classification guides that contain RD or FRD topics must be reviewed at least once every 5 years to ensure consistency with DOE classification policies and revised as necessary.

14-402. Requesting Guidance. Classification guides may be requested either from the DOE OCIC or the appropriate DOJ component. The RD Management Official may be contacted for assistance with this process.

Section 5.
Classifying RD and FRD Documents

14-500. Authority. Only those individuals designated as RD Classifiers may classify RD and FRD documents using classification guides as the primary basis for their determinations and source documents when use of classification guides is not practical. RD Classifiers may classify only documents in subject areas in which they have programmatic expertise.

14-501. Review Requirements.

a. Any DOJ employee or DOJ contractor who originates or possesses a document in an RD or FRD subject area must submit the document to an RD Classifier for a classification review.

b. Any DOJ employee or DOJ contractor who originates or possesses a document in an RD or FRD subject area that is intended for public release must submit the document to the DOE OCIC for a classification review. The RD Management Official shall be contacted for assistance in coordinating this review.

14-502. Review Procedures.

a. RD Classifiers may classify a document if two pieces of unclassified information in the document reveal classified information when associated.

b. RD Classifiers may classify a document because a number of pieces of unclassified information considered together contain some added value such as completeness or comprehensiveness of the information which warrants classification.

14-503. Reviews of the RD and FRD Program. The DOE and DOJ shall consult periodically to ensure appropriate implementation of the RD and FRD program. Such consultations may result in DOE conducting an on-site review if DOE and the RD Management Official determine that such a review would be mutually beneficial or that it is necessary to remedy a problem.

14-504. Marking RD and FRD Documents. In addition to the markings required for NSI, RD and FRD documents shall be clearly marked to convey to the holder that it contains RD or FRD information. The required markings are detailed in Chapter 5, Section 8 of this manual.

14-505. Upgrading and Downgrading. RD Classifiers may upgrade or downgrade the classification level of RD or FRD documents in accordance with joint DOE-DOJ classification guides or DOJ guides coordinated with the DOE. RD Classifiers may not upgrade or downgrade the category of RD or FRD documents.

Section 6.
Declassifying RD and FRD Documents

14-600. Declassification Procedures.

a. Documents containing RD or FRD are never automatically declassified. Such documents remain classified until an authorized individual takes positive action to declassify them. Under the Atomic Energy Act, no date or event for automatic declassification ever applies to RD/FRD documents, even if such documents also contain National Security Information (NSI).

b. Only designated individuals in DOE may declassify documents containing RD. The RD Management Official shall be contacted for assistance in obtaining a declassification review from the DOE OCIC.

c. Only designated individuals in DOE or appropriate individuals in the DoD may declassify documents containing FRD information using joint DoD-DOE classification guides or DoD guides which have been coordinated with the DOE. The RD Management Official shall be contacted for assistance in obtaining a declassification review from the DOE OCIC or appropriate DoD organization.

d. DOE and DoD (FRD only) can grant individual authority to declassify RD or FRD documents on a case-by-case basis. Contact the RD Management Official who will assist in obtaining this authority for individuals who have demonstrated a need to declassify RD and FRD documents.

Section 7.
Administrative Policies and Procedures

14-700. Submitting Information that may be RD. Any individual with authorized access to RD who possesses information that they believe may be RD must submit the information to an RD Classifier for evaluation. If no classification guidance can be applied to the information, but the information meets the RD definition and appears to be

potentially sensitive, then the RD Classifier must forward the information to the DOE OCIC for a determination. Information forwarded must be protected as Confidential Restricted Data at a minimum. The RD Management Official may be contacted for assistance with this process.

14-701. Proposals for Declassifying RD and FRD. Any individual with authorized access to RD or FRD who possesses information that they believe should be declassified must forward such proposal for declassification to the DOE OCIC for evaluation. The RD Management Official may be contacted for assistance with this process.

14-702. Suggestions or Complaints about RD and FRD Classification or Declassification Policies and Procedures. Any individual with a suggestion or complaint about RD or FRD classification or declassification policies and procedures should direct their suggestion or complaint to SO-10.21/Germantown Building, U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, D.C. 20585-1290. Correspondence should include a description of the issue or problem, the suggestion or complaint, all applicable background information, and an address for the response.

14-703. Request for Exemption to Procedural Requirements. When necessary, the RD Management Official may request an exemption to procedural requirements contained in 10 CFR Part 1045. Such request must be made in writing to the DOE OCIC and must describe the exemption requested, a justification for the exemption, and a proposed alternate or equivalent means of meeting the requirement.

14-704. Challenges to Classification. Any individual with authorized access to RD or FRD may challenge an RD/FRD classification with the RD Classifier who made the determination. Under no circumstances shall the individual be subject to retribution for making such a challenge. The RD Classifier must respond to the challenge within 90 days. If no response is received within 90 days or if the response by the RD Classifier does not satisfy the individual making the challenge, the individual may submit an initial appeal to the DOE OCIC, who must respond within 90 days. If the response by the DOE OCIC does not satisfy the individual making the challenge, the individual may submit a final appeal to the DOE Director of Security.

14-705. Preparing a Classified Addendum. To maximize the amount of information available to the public, the originator of a document containing RD or FRD information should include the unclassified portions in the primary document and should separate the RD or FRD portions into attachments, appendixes, or supporting documents. If such separation is not practical and there is significant public interest in the document, the originator is encouraged to prepare an unclassified version. When documents contain environmental, safety, or health information and a separate unclassified version cannot be prepared, document originators are encouraged to provide a publically releasable rationale for the classification of the document.

14-706. Responding to Freedom of Information Act (FOIA) and Mandatory Review Requests. A document containing RD information that is requested under the FOIA or the mandatory review provisions of Executive Order 13526 must be forwarded to the DOE OCIC for review. A document containing FRD information that is requested under the FOIA or mandatory review provisions must be forwarded to either the DOE OCIC or the appropriate DoD organization.

14-707. Systematic Review of RD and FRD Documents. DOJ components with RD and FRD documents must coordinate with the DOE OCIC to have the documents systematically reviewed. Contact the RD Management Official to coordinate the requesting of a review by the DOE or DoD (FRD only). The priority for requesting a systematic review should be based on the degree of public or researcher interest and likelihood of declassification upon review.

14-708. Unmarked Documents. Any individual who is reviewing documents under the automatic declassification or systematic review provisions of Executive Order 13526, or for any other reason (e.g., FOIA or mandatory review), may find documents they suspect contain RD or FRD information even through they are not so marked. Such documents are not subject to automatic declassification and must be sent to an RD Classifier for review.

14-709. No Comment Policy. Authorized holders of RD and FRD must not confirm or expand upon the classification status or technical accuracy of classified information in the public domain. Unauthorized disclosure of classified information does not automatically result in the declassification of that information.

14-710. Sanctions. Any knowing, willful, or negligent action that results in the misclassification of information, documents, or material violates this Chapter and may result in criminal, civil, and/or administrative penalties depending on the nature and severity of the action as determined by appropriate authority. Other violations of the policies and procedures contained in this chapter may be grounds for administrative sanctions as determined by appropriate authority.

Chapter 15
Reporting of Security Classification Management Program Data

Section 1.
Introduction

15-100. General. The statistics associated with the security classification program for components that create or handle classified information must be reported annually to the Information Security Oversight Office (ISOO) in accordance with Executive Order 13526. This information is included in an annual ISOO report to the President.

15-101. Responsibilities.

a. The Department Security Officer (DSO) shall work closely with the Security Programs Manager (SPM) to ensure that the most accurate statistics are collected for each of the categories identified below. Standard Form 311 (SF-311) "Agency Security Classification Management Program Data" shall be used for reporting this data.

b. Each component shall provide the security classification management program data for the previous fiscal year to the DSO by November 1, of each year.

c. The DSO will review the data for consistency and compile the data for the DOJ report.

Section 2.
Classification Program Management Categories.

15-200. General. Statistics for security classification program management data must be reported under one of the categories listed below. In some instances, the DSO already may have the data for a particular category and the SPM will be advised to disregard collecting that data.

15-201. Officials with Original Classification Authority (OCA). Officials with Original Classification Authority must include:

a. The number of individuals whose highest level of OCA is TOP SECRET;

b. The number of individuals whose highest level of OCA is SECRET; and

c. The number of individuals whose highest level of OCA is CONFIDENTIAL.

15-202. Original Classification Decisions.

a. Original classification decisions should include information on original classification decisions contained in products for dissemination or retention, regardless of the media or whether produced in electronic form. See Table 1 for examples of counting classification decisions. Do not count reproductions or copies or products classified by another organization. When possible, use an actual count for determining the number of original decisions. If an actual count is not possible, the sampling method discussed in Table 2 should be used to estimate original classification decisions. Components using the sampling method must annotate that fact in Part 1, Explanatory Comments, of their SF-311 report.

b. This count includes all products that are not necessarily on paper, such as, but not limited to, electronic presentations, e-mail; official correspondence or memoranda; photographs; reports and/or intelligence products; web pages; wiki articles and blog articles; and inputs and outputs from database records.

c. E-mail. Count only the first classified e-mail when after dissemination no additional classified information is added in the replies or forwards. Replies and forwards that include additional classified information should be counted in addition to the first classified e-mail. Do not count unclassified e-mails that are created on a system that is certified to handle classified information. Do not count e-mail that is merely a transmittal vehicle for a classified attachment and contains no classified information itself. Only count classified attachments that are originated by your component.

d. Web pages. Count web pages containing classified information created during the reporting period only once regardless of the number of times it was modified or updated. However, count only those web pages hosted by your component.

e. Blogs. Count every individual blog entry that constitutes a classification action. However, count only those blogs entries for blogs hosted by your component.

f. Wiki Articles. Count wiki articles containing classified information created during the reporting period only once regardless of the number of times it was modified or updated. However, count only those wiki articles hosted by your component.

g. Instant Messages. Instant messages should not be counted.

(1) The number of original TOP SECRET classification decisions with declassification instructions of 10 years or less;

(2) The number of original TOP SECRET classification decisions with declassification instructions ranging from over 10 years to 25 years;

(3) The number of original SECRET classification decisions with declassification instructions of 10 years or less;

(4) The number of original SECRET classification decisions with declassification instructions ranging from over 10 years to 25 years;

(5) The number of original CONFIDENTIAL classification decisions with declassification instructions of 10 years or less;

(6) The number of original CONFIDENTIAL classification decisions with declassifications instructions ranging from over 10 years to 25 years.

15-203. Derivative Classification Decisions.

a. Derivative classification decisions should include information on derivative classification decisions contained in products for dissemination or retention, regardless of the media or whether produced in electronic form. See Table 1 for examples of counting classification decisions. Do not count reproductions or copies. When possible, use an actual count for determining the number of derivative decisions. If an actual count is not possible, the sampling method discussed in Table 2 should be used to estimate derivative classification decisions. Components using the sampling method must annotate that fact in Part 1, Explanatory Comments, of their SF-311 report.

b. This count includes all products that are not necessarily on paper, such as, but not limited to, electronic presentations; e-mail; official correspondence or memoranda; photographs; reports and/or intelligence products; web pages; wiki articles and blog articles; and inputs and outputs from database records.

c. E-mail. Count only the first classified e-mail when after dissemination no additional classified information is added in the replies or forwards. Replies and forwards that include additional classified information should be counted in addition to the first classified e-mail. Do not count unclassified e-mails that are created on a system that is certified to handle classified information. Do not count e-mail that is merely a transmittal vehicle for a classified attachment and contains no classified information itself. Only count classified attachments that are originated by your component.

d. Web pages. Count web pages containing classified information created during the reporting period only once regardless of the number of times it was modified or updated. However, count only those web pages hosted by your component.

e. Blogs. Count every individual blog entry that constitutes a classification action. However, count only those blogs entries for blogs hosted by your component.

f. Wiki Articles. Count wiki articles containing classified information created during the reporting period only once regardless of the number of times it was modified or updated. However, count only those wiki articles hosted by your component.

g. Instant Messages. Instant messages should not be counted.

(1) The number of derivative TOP SECRET classifications;

(2) The number of derivative SECRET classifications; and

(3) The number of derivative CONFIDENTIAL classifications.

15-204. Mandatory Declassification Review Requests and Appeals. A request is an individual review request or appeal, regardless of the number of documents or pages to be reviewed as part of the request. Report only requests for your component in which your component is responsible for the final decision. Provide an explanation where the number of requests or appeals carried forward between reporting periods changes.

a. The number of requests carried over from the previous reporting period;

b. The number of new requests received during the reporting period;

c. The number of requests carried over to the next reporting period;

d. The number of appeals carried over from the previous reporting period;

e. The number of new appeals received during the reporting period; and

f. The number of appeals carried over to the next reporting period.

15-205. Mandatory Declassification Review Decisions in Pages. Mandatory declassification review decisions in pages must include:

a. The number of requested pages that were declassified in full;

b. The number of requested pages that were declassified in part;

c. The number of requested pages that were denied declassification;

d. The number of appealed pages that were declassified in full;

e. The number of appealed pages that were declassified in part; and

f. The number of appealed pages that were denied declassification.

15.206. Automatic, Systematic, and Discretionary Declassification Reviews. Discretionary reviews are those decisions by an OCA or official with declassification authority that are not performed under the automatic, systematic, or mandatory review programs. Automatic, systematic, and discretionary declassification reviews must include:

a. The number of pages reviewed that were subject to automatic declassification under section 3.3 of Executive Order 13526;

b. The number of pages declassified under section 3.3 of Executive Order 13526;

c. The number of pages reviewed that were subject to systematic declassification under section 3.4 of Executive Order 13526;

d. The number of pages declassified under section 3.4 of Executive Order 13526;

e. The number of pages reviewed that were subject to discretionary declassification under section 3.1 of Executive Order 13526; and

f. The number of pages declassified under section 3.1 of Executive Order 13526.

15-207. Internal Agency Oversight. Internal agency oversight must include:

a. The number of inspections, surveys, or program reviews, covering any aspect of the security classification program completed during the reporting period. Only count significant efforts to self-inspect the classified information security program. Do not count minor inspections such as routine after-hours security checks;

b. The number of internal or external challenges processed by the component to the classification of information believed to be improperly classified or unclassified. Do not count requests received under the Freedom of Information Act or the Mandatory Declassification Review provisions of Executive Order 13526;

c. The number of challenges where the classification status was fully affirmed; and

d. The number of challenges where the classification status was overturned in whole or in part.

15–208. Classification Guides. Classification guides must include the number of security classification guides created by the component and currently in use. Additionally, annotate in the explanatory comments section the number of guides that have not been reviewed and/or updated during the last five years.

15-209. Explanatory Comments. This section should be used to elaborate on any aspect of the report or provide a narrative for any significant changes in trends/numbers or large deviations from numbers submitted in the previous year's report.

a. Report when the sampling process outlined in Table 2 is used in developing the report.

Table 1: Examples of Counting Classification Decisions:		
Paper Environment	Electronic Environment	How to Count
A report contains classified information derived from a classified source and is photocopied and distributed to 30 recipients.	An e-mail contains classified information derived from a classified source and is disseminated to 20 recipients, and then forwarded on to 10 more recipients.	Count as one classification decision. Do not count as 30 or 31 classification decisions.
An unclassified internal memo is drafted in response to a classified Inspector General (IG) report. The IG report will be distributed as an attachment to the unclassified internal memo.	An unclassified transmittal e-mail is drafted in response to a classified IG report. The IG report will be distributed as an electronic attachment to the unclassified e-mail.	Do not count as a classification decision. A classification decision was already counted at the creation of the classified IG report. The e-mail must be protected as classified (classified transmittal), but does not warrant a classification count.

Table 2: Steps for Sampling Classification Decisions:	
1. Define the Total Population	This total population estimate should include all personnel making classification decisions under your component's authority.
2. Define the Sampling Population	After identifying the total population of classifiers, a sampling population must be defined. Sample a percentage of the total population and then estimate the total number or original and derivative classification decisions component-wide. The percentage used to identify the sampling population is ten percent.
3. Collect Data of Sample Population	Request each classifier, derivative and original, to provide the number of classification decisions for a two-week period during the fiscal year. The manner in which the data is collected is at the discretion of the component; however, components may employ a survey via e-mail that is disseminated to the entire sampling population.

Chapter 16
Controlled Unclassified Information

RESERVED

Annex A
Glossary Of Security Terms

ACCESS. The ability and opportunity to gain knowledge of classified information.

ACCESS CONTROL. The process of limiting access to the resources of a system to only authorized persons, programs, processes, or other systems. Synonymous with controlled access and limited access.

ACCREDITATION. A formal declaration by an accrediting authority that a computer system or facility is approved to operate in a particular security mode using a prescribed set of safeguards.

ACCREDITING AUTHORITY. The official who has the authority to decide to accept the security safeguards prescribed for a computer system or facility, or official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The Senior Executive Service personnel designated by the Component Head are authorized accrediting authorities.

ADVERSE INFORMATION. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

APPLICANT. A person, other than an employee, who has received an authorized conditional offer of employment for a position that requires access to classified information.

AUTHORIZED PERSON. A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personnel clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an AUTHORIZED PERSON rests with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient.

AUDIT TRAIL. A chronological record of system activities that enables the reconstruction and examination of the sequence of events and/or changes in an event.

AUTOMATIC DECLASSIFICATION. The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority; or the expiration of a maximum time frame for duration of classification established under Executive Order 13526.

AUTHENTICATE. To verify the identity of a user, device, or other entity, often as a prerequisite to allowing access to resources in a computer system.

CERTIFICATION. The comprehensive security test and evaluation of the technical and nontechnical security features of a computer system and other safeguards applicable to that system**,** made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

CLASSIFICATION. The act or process by which information is determined to be classified information.

CLASSIFICATION GUIDANCE. Any instruction or source that prescribes the classification of specific information.

CLASSIFICATION GUIDE. 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.

CLASSIFIED CONTRACT. Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of precontract activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other Government Contracting Activity program or project which requires access to classified information by a contractor.

CLASSIFIED DOCUMENT. Any recorded classified information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

CLASSIFIED NATIONAL SECURITY INFORMATION (or "CLASSIFIED INFORMATION"). Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

COMMUNICATIONS SECURITY (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such communications. Communications Security includes crypto security, transmission security, and physical security of COMSEC material.

COMPILATIONS OF CLASSIFIED INFORMATION. An aggregation of pre-existing unclassified items of information. Items of information which 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 13526; and is not otherwise revealed in the individual items of information.

a. Document: When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers.

b. Portions of a document: If a document contains certain portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on the page, and a statement shall be added to the page, or to the document, to explain the classification of the combination or association to the holder.

COMPONENT. Any Office, Board, Division, or Bureau that is part of the Department of Justice.

COMPROMISE. The disclosure of classified information to persons not authorized access.

COMPUTER. Synonymous with computer system.

CONFIDENTIAL. Level of classification 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.

CONTINGENCY PLAN. An emergency response plan, backup operations plan, post-disaster recovery plan, maintained by an activity as a part of a security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan.

CONUS. The conterminous United States (the 48 contiguous States and the District of Columbia).

DAMAGE TO THE NATIONAL SECURITY.
Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

DD FORM 254. The completed DD Form 254 is the basic document conveying to a contractor the contract security classification specifications and guidelines for the classification, regrading and downgrading of documents used in the performance of a classified contract.

DECLASSIFICATION. The authorized change in the status of information from classified information to unclassified information.

DECLASSIFICATION AUTHORITY. The official who authorized the original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority in writing by the agency head or the senior agency official.

DEGAUSS. To destroy information contained in magnetic media by subjecting that media to high intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

DEGAUSSER. An electrical device that generates a magnetic field for the purpose of degaussing magnetic storage media.

DERIVATIVE CLASSIFICATION. 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.

DOWNGRADE. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

EMPLOYEE. 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.

ENCRYPTION. The process of transforming data to an unintelligible form in order to conceal its meaning in such a way that the original data cannot be obtained without using the inverse decryption process.

ENVIRONMENT. The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

FACILITY (SECURITY) CLEARANCE. An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

FILE SERIES. Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

FOREIGN AREA. Any location other than CONUS and overseas US locations, i.e., other than CONUS, Alaska,

Hawaii, Puerto Rico, the US Virgin Islands, Guam, American Samoa, Midway Islands, the Northern Mariana Islands, Johnston Atoll, or Wake Island.

FOREIGN GOVERNMENT INFORMATION (FGI). 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; information produced by the United States 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 information received and treated as "Foreign Government Information" under the terms of an executive order that is a predecessor of Executive Order 13526.

FOREIGN POWER. Means -

a. a foreign government or any component thereof, whether or not recognized by the United States;

b. a faction of a foreign nation or nations, not substantially composed of United States persons;

c. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

d. a group engaged in international terrorism or activities in preparation thereof;

e. a foreign-based political organization, not substantially composed of United States persons; or

f. an entity that is directed and controlled by a foreign government or governments.

FORMERLY RESTRICTED DATA. Means classified information jointly determined by DOE and the DoD to be related primarily to the military utilization of nuclear weapons and removed (by transclassification) from the RD category pursuant to section 142(d) of the Atomic Energy Act.

FREEDOM OF INFORMATION ACT (FOIA). Provides that any person has a right of access to Federal Agency records, except to the extent that such records are protected form disclosure by statutory exemptions.

IDENTIFICATION. The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

INDIVIDUALLY ACCOUNTABLE. The ability to associate positively the identity of a user with the time, method, and degree of access to a system.

INFORMATION. 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.

INFORMATION RESOURCES MANAGEMENT (IRM). The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies, including the management of information and related resources, such as federal information processing resources.

INTEGRITY. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

LEAST PRIVILEGE. The principle that requires that each person be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

MANDATORY DECLASSIFICATION REVIEW. The review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of Executive Order 13526.

MULTIPLE SOURCES. Means two or more source documents, classification guides, or a combination of both.

NATIONAL SECURITY. Means the national defense or foreign relations of the United States.

NEED FOR ACCESS. 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.

NEED-TO-KNOW. A determination within the executive branch in accordance with directives issued pursuant to the Order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

NETWORK. A system of two or more computers that can exchange data or information. Communic
ations medium and all components attached to that medium whose responsibility is the transference of information. Such components may include automated information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

NONDISCLOSURE AGREEMENT. Agreement signed by recipient of classified information certifying that classified information, derived in the course of official duties, will not be divulged to unauthorized persons.

ORIGINAL CLASSIFICATION. The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

ORIGINAL CLASSIFICATION AUTHORITY. An individual authorized in writing, either by the President, or by

agency heads or other officials designated by the President, to classify information in the first instance.

OVERWRITE PROCEDURE. Process which removes or destroys data recorded on a computer storage medium by writing patterns of data over, or on top of, the data stored on the medium.

PASSWORD. A protected and private character string used to authenticate an identity.

PERSONNEL SECURITY CLEARANCE. An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

PHYSICAL SECURITY. The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and information.

PORTABLE ELECTRONIC DEVICE (PED). Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

PRIVACY ACT (5 U.S.C. 552a). The Privacy Act regulates the collection, maintenance, use and dissemination of personal information by Federal Government Agencies.

PROTECTED DISTRIBUTION SYSTEM. Wireline or fiber-optic distribution systems used to transmit unencrypted classified National Security Information through an area of lesser classification or control.

PURGE. The removal of data from computer system storage devices in such a way that there is assurance, proportional to the sensitivity of the data, that the data cannot be reconstructed. Purging is used when the secure physical environment will not be maintained. Media scheduled to be released from a secure facility to a non-secure facility must be purged.

REPRESENTATIVE OF FOREIGN INTEREST. An individual or group that acts on behalf of a foreign government or enterprise.

RESIDUAL RISK. The portion of risk that remains after security measures have been applied.

RESTRICTED DATA. Means a kind of classified information that consists of all data concerning the following, but not including data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act:

a. Design, manufacture, or utilization of atomic weapons;

b. Production of special nuclear material; or

c. Use of special nuclear material in the production of energy.

RISK ANALYSIS. The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

RISK MANAGEMENT. The total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

SAFEGUARDS. See, security safeguards.

SECRET. Level of classification 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.

SECURITY in DEPTH. A determination made by the DSO that a security program consists of layered and complimentary security controls sufficient to deter and detect unauthorized entry and movement within a facility.

SECURITY REQUIREMENTS. The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

SECURITY SAFEGUARDS. The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include, but are not limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. Also called safeguards.

SECURITY VIOLATION. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; to classify or continue the classification of information contrary to the requirements of the Order or its implementing directives; or to create or continue a special access program contrary to the requirements of the Order.

SENSITIVE INFORMATION. Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

SENSITIVE COMPARTMENTED INFORMATION (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

SERVICING PERSONNEL SECURITY OFFICE. The office that holds and maintains an individual's security record.

SINGLE TRUSTED SYSTEM. An approach in which a network is accredited as a single computer system.

SOURCE DOCUMENT. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

SPECIAL ACCESS PROGRAM. 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.

SPECIAL CATEGORY (SPECAT). Restrictive label that has been applied to both classified and unclassified information, thereby increasing the requirements for protection of, and restricting access to, the information.

STANDARD SECURITY PROCEDURES. Step-by-step security instructions tailored to users and operators of computer systems which process sensitive or classified information.

SYSTEMATIC DECLASSIFICATION REVIEW. The review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with Chapter 33 of Title 44, United States Code.

TEMPEST. The study and control of electronic signals emitted by electrical equipment.

TOP SECRET. Level of classification 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.

TRANSCLASSIFICATION. When information has been removed from the RD category by a joint determination of DOE and DoD and placed in the FRD category in accordance with section 142d of the Atomic Energy Act.

UNAUTHORIZED DISCLOSURE. A communication or physical transfer of classified information to an unauthorized recipient.

VIRUS. Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

VULNERABILITY. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

USER IDENTIFICATION. A unique symbol or character string that is used by a system to identify a specific user.

Annex B
Acronym List

AAG/A	Assistant Attorney General for Administration
ACO	Sensitive Compartmented Information Facility Alternate Control Officer
AG	Attorney General
ANACI	Access National Agency Check with Inquiries
ARC	Access Review Committee
BI	Background Investigation
CAGE	Commercial and Government Entity
CCI	Controlled Cryptographic Item
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CMCS	COMSEC Material Control System
CMS	Contractor Monitoring Station
CNSS	Committee on National Security Systems
COMSEC	Communications Security
COR	Central Office of Record
CPU	Central Processing Unit
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
DAG	Deputy Attorney General
DCID	Director Central Intelligence Directive
DCII	Defense Clearance & Investigations Index
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOJCERT	DOJ Computer Emergency Response Team
DOS	Department of State
DRC	Department Review Committee
DSO	Department Security Officer
DSS	Defense Security Service
EO	Executive Order
EPL	Evaluated Products List
FAA	Facility Access Approval
FBI	Federal Bureau of Investigation
FED STD	Federal Standard
FFC	Fixed Facility Checklist
FGI	Foreign Government Information
FIPS	Federal Information Processing Standards
FOCI	Foreign Ownership, Control or Influence
FOIA	Freedom of Information Act
FPGA	Field Programmable Gate Array
FRD	Formerly Restricted Data
FRUS	Foreign Relations of the United States
GSA	General Services Administration
IA	Information Assurance
ICD	Intelligence Community Directive
IDE	Intrusion Detection Equipment
IDS	Intrusion Detection System
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
ISPG	Information Security Policy Group
ISSO	Information Systems Security Officer
IT	Information Technology
ITSS	Information Technology Security Staff
JMD	Justice Management Division
JSOC	Justice Security Operations Center
KMC	Key Management Center
KMM	Keyboard/Monitor/Mouse
KVM	Keyboard/Video/Mouse
LSG	Litigation Security Group
MDR	Mandatory Declassification Review
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Agency Check
NACLC	National Agency Check with local agency checks and credit record
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NCIRES	National COMSEC Incident Reporting and Evaluation System
NdA	Nondisclosure Agreement
NDC	National Declassification Center
NIAP	National Information Assurance Partnership
NID	National Interest Determination
NISP	National Industrial Security Program

NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSI	National Security Information
NTISSI	National Telecommunications and Information Systems Security Instruction
OADR	Originating Agency's Determination Required
OCA	Original Classification Authority
OCIC	Office of Classification and Information Control
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OIP	Office of Information and Privacy
OISSO	Office of Information Safeguards and Security Oversight
OMB	Office of Management and Budget
OPF	Official Personnel File
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
OPSEC	Operations Security
PCL	Personnel Security Clearance
PDS	Protected Distribution System
PED	Portable Electronic Device
RD	Restricted Data
RFK	Robert F. Kennedy
SAO	Senior Agency Official
SAP	Special Access Program
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCO	Sensitive Compartmented Information Facility Control Officer
SEPS	Security and Emergency Planning Staff
SF	Standard Form
SFU	Secure Facility Unit
SII	Security/Suitability Investigations Index
SNM	Special Nuclear Material
SOP	Standard Operating Procedures
SPECAT	Special Category
SPM	Security Programs Manager
SRR	Security Review Report
SSA	Special Security Agreement
SSC	Special Security Center
SSBI	Single Scope Background Investigation
SSBI-PR	Single Scope Background Investigation - Periodic Review
SSO	Special Security Officer
STE	Secure Telephone Equipment
TAIS	Telecommunications and Automated Information System
TFNI	Transclassified Foreign Nuclear Information
TPI	Two Person Integrity
TSA	Transportation Security Administration
TSCM	Technical Surveillance Countermeasures
UL	Underwriters Laboratory
URL	Uniform Resource Locator
USSAN	United States Security Authority, NATO
VAL	Visit Authorization Letter
WMD	Weapons of Mass Destruction

Annex C
Adjudicative Guidelines For Determining Eligibility For Access To Classified Information and to Sensitive Compartmented Information and Special Access Programs

Section 1.
Introduction

The following adjudicative guidelines are to be used for all Department of Justice (DOJ) personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by all DOJ components in all final clearance determinations. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitments to the United States, including the commitment to protect classified information, and any other compelling loyalty. Access decisions also take into account a person's reliability, untrustworthiness and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets as the most effective means of policing them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

Section 2.
The Adjudicative Process

a. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1.) The nature, extent, and seriousness of the conduct;

(2.) The circumstances surrounding the conduct, to include knowledgeable participation;

(3.) The frequency and recency of the conduct;

(4.) The individual's age and maturity at the time of the conduct;

(5.) The voluntariness of participation;

(6.) The presence or absence of rehabilitation and other permanent behavioral changes;

(7.) The motivation for the conduct;

(8.) The potential for pressure, coercion, exploitation, or duress; and

(9.) The likelihood of continuation or recurrence.

b. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security.

c. The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

(1.) GUIDELINE A: Allegiance to the United States;

(2.) GUIDELINE B: Foreign Influence;

(3.) GUIDELINE C: Foreign Preference;

(4.) GUIDELINE D: Sexual Behavior;

(5.) GUIDELINE E: Personal Conduct;

(6.) GUIDELINE F: Financial Considerations;

(7.) GUIDELINE G: Alcohol Consumption;

(8.) GUIDELINE H: Drug Involvement;

(9.) GUIDELINE I: Psychological Conditions;

(10.) GUIDELINE J: Criminal Conduct;

(11.) GUIDELINE K: Handling Protected Information;

(12.) GUIDELINE L: Outside Activities;

(13.) GUIDELINE M: Misuse of Information Technology Systems

d. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

e. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1.) Voluntarily reported the information;

(2.) Was truthful and complete in responding to questions;

(3.) Sought assistance and followed professional guidance, where appropriate;

(4.) Resolved or appears likely to favorably resolve the security concern;

(5.) Has demonstrated positive changes in behavior and employment; and

(6.) Should have his or her access temporarily suspended pending final adjudication of the information.

f. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

To access the December 29, 2005, Adjudicative Guidelines For Determining Eligibility For Access to Classified Information in its entirety, to include concerns and mitigating factors for each Guideline, click on the following link, http://www.rjhresearch.com/ADR/adjguidelines/adjguidframeset.htm

To access the Intelligence Community Policy Guidance Number 704.2, Personnel Security Adjudicative Guidelines For Determining Eligibility For Access To Sensitive Compartmented Information And Other Controlled Access Program Information, effective October 2, 2008, in its entirety, to include concerns and mitigating factors for each Guideline, click on the following link, http://www.dni.gov/electronic_reading_room/ICPG_704_2.pdf

Annex D
Investigative Standards For Background Investigations For Access To Classified Information

Section 1.
Introduction

D-100. Introduction. The following investigative standards are established for all Department of Justice (DOJ) employees, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs) and are to be used by all DOJ components as the investigative basis for clearance eligibility determinations.

D-101. Additional Coverage. Nothing in these standards prohibits the DOJ or a component from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or re-investigation.

Section 2.
General Information

D-200. The Two Standards. There are two standards (Table 1 at the end of this Annex summarizes when to use each one).

a. The investigation and re-investigation standards for Department of Energy (DOE) "L" access authorizations and for access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by Section 4.4 of Executive Order 13526);

b. The investigation standard for DOE "Q" access authorizations and for access to TOP SECRET (including TOP SECRET SAPS) and SCI.

D-201. Exception to Periods of Coverage. Some elements of standards specify a period of coverage (e.g., ten years). Where appropriate, such coverage may be shortened to the period from the subject's eighteenth birthday to the present or to two years, whichever is longer.

D-202. Expanding Investigations. Investigations and re-investigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and executive orders.

D-203. Transferability. Investigations that meet, or exceed, the requirements of a given standard, are favorably adjudicated, are current (less than 5 years old), and meet DOJ Background Investigation (BI) requirements shall be accepted by the DOJ. Components must ensure that a new security questionnaire is not completed or the conduct of duplicative checks does not occur. Only additional investigative and adjudicative procedures may be completed with approval from the Suitability and Security Clearance Performance Accountability Council established by Executive Order 13467 of June 30, 2008. For example, a DEA applicant may complete a DEA drug use statement.

D-204. Breaks in Service. If a person who requires access has been retired or separated from U.S. Government employment for less than two years, is the subject of a favorably adjudicated investigation that is otherwise current and the person certifies in writing that there has been no change in the relevant information since the last BI, the component re-granting the access will only initiate an FBI fingerprint check. A re-investigation is not required unless the review indicates the person may no longer satisfy the access standards of this manual.

D-205. The National Agency Check (NAC). The NAC is a part of all investigations and re-investigations. It consists of a review of:

a. Investigative and criminal history files of the FBI, including a technical fingerprint search;

b. OPM's Security/Suitability Investigations Index;

c. DoD's Defense Clearance and Investigations Index; and

d. Such other national agencies (e.g., Central Intelligence Agency, Department of Homeland Security, U.S. Citizenship & Immigration Services) as appropriate to the individual's background.

Section 3.
Standard for Access to Confidential and Secret Information.

D-300. Applicability. This standard applies to initial investigations for access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by section 4.4 of Executive Order 13526), and for "L" access authorizations.

D-301. When to Re-investigate. The re-investigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation or re-investigation. (The table at the end of this Annex reflects the specific investigative requirements.)

D-302. Investigative and Re-investigative Requirements. The Access National Agency Check with Inquiries (ANACI) is the required initial investigation for Federal employees and contractors for clearance access at the Confidential and Secret levels. The National Agency Check with Local Agency

Checks (NACLC) is the required reinvestigation for Federal employees and contractors for clearance access at these clearance levels.

D-303. Expanding the Investigation. The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

Section 4.
Standard for Access to Top Secret and Sensitive Compartmented Information
(Single Scope Background Investigation (SSBI)).

D-400. Applicability. This standard applies to initial investigations for access to TOP SECRET (including TOP SECRET SAPs) and SCI; and for DOE "Q" access authorizations.

D-401. Expanding the Investigation. The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to co-habitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Section 5.
Standard for Periodic Reinvestigations.
(Phased Periodic Reinvestigation (PPR) or Single Scope Background Investigation--Periodic Reinvestigation (SSBI-PR)).

D-500. Applicability. This standard applies to re-investigations for access to TOP SECRET (including TOP SECRET SAPs) and SCI; and for DOE "Q" access authorizations.

D-501. When to Re-investigate. The re-investigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation (see the table at the end of this Annex).

D-502. Expanding the Re-investigation. The re-investigation may be expanded as necessary. For example, if a PPR is initiated and questionable or derogatory information surfaces, the PPR will automatically expand to a full SSBI-PR. In addition, an SSBI-PR may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to co-habitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Section 6.
Investigative Standards for Temporary Eligibility for Access.

D-600. Introduction. The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, Access to Classified Information, are established for all DOJ employees, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

D-601. Temporary Eligibility for Access.

a. Based on a justified need meeting the requirements of Section 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process.

b. The temporary eligibility for access shall be valid until completion of the investigation and adjudication or for a period not to exceed 180 days, whichever is less.

c. The temporary eligibility for access may be terminated by the granting authority at any time based on unfavorable information identified in the course of the investigation.

D-602. Temporary Eligibility for Access at the CONFIDENTIAL and SECRET Levels. As a minimum, such temporary eligibility requires completion of the e-QIP SF-86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited ANACI for an initial investigation and an expedited NACLC for a reinvestigation, a credit check, and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the FBI.

D-603. Temporary Eligibility for Access at the TOP SECRET and SCI Levels.

a. For someone who is the subject of a favorable investigation not meeting the investigative standards for access at the TOP SECRET, SCI, or "Q" levels, temporary eligibility requires completion of the e-QIP SF-86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, a credit check, and submission of an expedited SSBI.

b. For someone who is not the subject of a current, favorable personnel or personnel-security investigation of any kind. As a minimum, such temporary eligibility requires completion of the e-QIP SF-86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited SSBI, a credit check, and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the FBI and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII). A National Crime Information Center (NCIC) check may be used pending completion of the FBI name/fingerprint checks.

D-604. Additional Requirements.

a. Temporary eligibility for access must satisfy these minimum investigative standards. The DSO may establish additional requirements based on the sensitivity of the particular**,** identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access; however, no additional requirements shall exceed the common standards for background investigations (BIs) developed under Section 3.2(b) of Executive Order 12968, or any future revisions to the BI common standards.

b. Temporary eligibility for access is valid only within the DOJ component that requested it and at other DOJ components and agencies who expressly agree to accept it and acknowledge the understanding of its investigative basis. For example, the Department of Energy will not grant an "L" or "Q" clearance based on a temporary clearance.

c. Temporary eligibility for access shall include a written justification to be maintained in the personnel security records.

TABLE 1. Which Investigation to Request

ACCESS LEVEL			FORM	TYPE OF INVESTIGATION	
CONF	SECRET "L"	TS "Q"	SF 86	INITIAL BACKGROUND INVESTIGATION (BI) REQUIRED	RE-INVESTIGATION (RI) REQUIRED
		X	X	SSBI - Single Scope BI (10 year scope)	PPR (Phased Periodic Reinvestigation) or SSBI-PR - SSBI Periodic RI (5 yr scope)
X	X		X	ANACI – Access National Agency Check w/Inquiries	NACLC – National Agency Check with Local Agency Checks

Annex E
Guidelines for Construction of Open Storage Areas

Section 1.
Introduction.

When the volume or bulk of classified material is such that the use of security containers is not practical, the construction of an open storage area must be considered.

a. When a component determines that an open storage area is required, the component Security Programs Manager (SPM) should contact the Department Security Officer (DSO) to request a survey of the proposed facility.

b. After the construction of an open storage area is approved by the DSO, a Standard Operating Procedure (SOP) for this facility must be developed and provided to the DSO.

c. Upon completion of the construction phase of the open storage area, but before the facility is used, the facility must be inspected and an open storage area checklist completed before the written approval will be provided by the DSO.

d. Any changes to the construction of the open storage area or major modifications of the area which require major structural changes must be approved in writing by the DSO before the modifications are initiated.

Section 2.
General.

This Section describes the construction requirements for open storage areas. Construction shall conform to the requirements of this Annex or, with DSO approval, to the standards of Intelligence Community Directive (ICD) 705 (Sensitive Compartmented Information Facilities.)

Section 3.
Construction Requirements for Open Storage Areas.

These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used for evaluating the adequacy of existing areas.

a. Only heavy duty builder's hardware shall be used in construction. Hardware accessible from outside the area shall be peened, pinned, brazed, or spot-welded to preclude removal.

b. Construction may be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, glass, and wire mesh, expanded metal, or other materials offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. If visual access is a factor, area barrier walls up to a height of 8 feet shall be of opaque or translucent construction.

c. The openings for windows which open, that are less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door) shall be fitted with 1/2-inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18-gauge expanded metal, or wire mesh securely fastened on the inside. When visual access of classified information is a factor, the windows shall be covered by any practical method, such as drapes, blinds, or painting or covering the inside of the glass. During non-working hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

d. Doors shall be substantially constructed of wood or metal. When windows, louvers, baffle plates, or similar openings are used, they shall be secured with 18-gauge expanded metal or with wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be covered. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet. Hinge pins that are exposed to the outer perimeter of the area shall have set screws or non-removable pins.

e. Entrance doors shall be secured with either an approved built-in combination lock, an approved combination padlock, or with an approved key-operated padlock. Other doors shall be secured from the inside with a panic bolt (for example, actuated by a panic bar); a dead bolt; a rigid wood or metal bar, (that shall preclude "springing") and shall extend across the width of the door and be held in position by solid clamps, preferably on the door casing; or by other means approved by the DSO consistent with relevant fire and safety codes.

f. Ceilings shall be constructed of plaster, gypsum wall board material, panels, hardboard, wood, plywood, ceiling tile, or other material offering similar resistance to and detection of unauthorized entry. Wire mesh, or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area may be used if visual access to classified material is not a factor.

g. When wall barriers do not extend to the true ceiling and a false ceiling is created, the false ceiling must be reinforced with wire mesh or 18-gauge expanded metal to serve as the true ceiling. When wire mesh or expanded metal is used, it must overlap the adjoining walls and be secured in a manner that precludes removal without leaving evidence of tampering. When wall barriers of an area do extend to the true ceiling and a false ceiling is added, there is no necessity for reinforcing the false ceiling. When there is a valid justification for not erecting a solid ceiling as part of the area, such as the use of overhead cranes for the movement of bulky equipment within the area, the contractor shall ensure that surreptitious entry cannot be

obtained by entering the area over the top of the barrier walls.

h. Where ducts, pipes, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry, (in excess of 96 square inches in area and over 6 inches in its smallest dimension) they shall be secured by 18-gauge expanded metal or wire mesh, or, by rigid metal bars 1/2-inch in diameter extending across their width, with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading. When wire mesh, expanded metal, or rigid metal bars are used, they must ensure that classified material cannot be removed through the openings with the aid of any type instrument. Expanded metal, wire mesh or rigid metal bars are not required if an Intrusion Detection System is used as supplemental protection.

Annex F
Intrusion Detection System Standards

Section 1.
General

This Section specifies the minimum standards for an approved Intrusion Detection System (IDS) when used as supplemental protection for TOP SECRET and SECRET material. The IDS shall be connected to, and monitored by, a central monitoring station. Alarm system installation shall conform to the requirements of this Annex or to the standards set forth in DCID 6/9 (Physical Security Standards for Sensitive Compartmented Information Facilities). The Department Security Officer (DSO) will approve contingency protection procedures in the event of IDS malfunction.

Section 2.
DSO Approval

DSO approval is required before installing an IDS. Approval of a new IDS shall be based on the criteria of DCID 6/9 or Underwriters Laboratory (UL) Standard 2050, as determined by the DSO. IDSs currently in use that do not meet either of these standards, such as those certified to meet Grade A service and those installed by a non-UL listed company, may continue in use.

Section 3.
Central Monitoring Station.

a. The central monitoring station may be located at the facility or a UL listed: (1) Contractor Monitoring Station (CMS) formerly called a proprietary central station; (2) Cleared commercial central station; (3) Cleared protective signal service station (e.g., fire alarm monitor); or (4) Cleared residential monitoring station. For the purpose of monitoring alarms, all provide an equivalent level of monitoring service.

b. Trained alarm monitors, cleared to the SECRET level, shall be in attendance at the alarm monitoring station at all times when the IDS is in operation.

c. The central monitoring station shall be required to indicate whether or not the system is in working order and to indicate tampering with any element of the system. Necessary repairs shall be made as soon as practical. Until repairs are completed, periodic patrols shall be conducted during non-working hours, unless a SECRET cleared employee is stationed at the alarmed site.

d. When an IDS is used, it shall be activated immediately at the close of business at the alarmed area or container. This may require that the last person who departs the controlled area or checks the security container notify the central monitoring station to set the alarm. A record shall be maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate shall be reported to the component Security Programs Manager (SPM). Such records shall be maintained for 30 days.

e. Records shall be maintained for 90 days indicating time of receipt of alarm; name(s) of security force personnel responding; time dispatched to facility/ area; time security force personnel arrived; nature of alarm; and what follow-up actions were accomplished.

Section 4.
Investigative Response to Alarms.

a. The following resources may be used to investigate alarms: proprietary security force personnel, central station guards, and a subcontracted guard service.

(1.) Trained proprietary security force personnel, cleared to the SECRET level and sufficient in number to be dispatched immediately to investigate each alarm, shall be available at all times when the IDS is in operation.

(2.) For a commercial central station, protective signaling service station, or residential monitoring station, guards dispatched shall be cleared only if they have the ability and responsibility to access the area or container(s) housing classified material; i.e., keys to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material.

(3.) Uncleared guards dispatched by a commercial central station, protective signaling service station, or residential monitoring station to an alarm shall remain on the premises until a designated, cleared representative of the facility arrives, or for a period of not less than 1 hour, whichever comes first. If a cleared representative of the facility does not arrive within 1 hour following the arrival of the guard, the central control station must provide the component SPM with a report of the incident that includes the name of the subscriber facility, the date and time of the alarm, and the name of the subscriber's representative who was contacted to respond. A report shall be submitted to the DSO within 24 hours of the next working day. (NOTE: The primary purpose of any alarm response team is to ascertain if intrusion has occurred and if possible assist in the apprehension of the individuals. If an alarm activation resets in a reasonable amount of time and no physical penetration of the area or container is visible, then entrance into the area or container is not required. Therefore, the initial response team may consist of uncleared personnel. If the alarm activation does not reset or physical penetration is observed, then a cleared response team must be dispatched. The initial uncleared response team must stay on station until relieved by the cleared response

team. If a cleared response team does not arrive within one hour, then a report to the DSO must be made by the close of the next business day.)

(4.) Subcontracted guards must be under contract with either the installing alarm company or the cleared facility.

b. The response time shall not exceed 5 minutes for Top Secret information stored in an approved open storage area, 15 minutes for Top Secret information stored in a GSA approved security container and 30 minutes for Secret information stored in a non-GSA approved container or an approved open storage area. (NOTE: The UL standard for response within the time limits is 80%. That is the minimum allowable on-time response rate. Anything less than 80% is unacceptable. However, in all cases, a guard or cleared employee must arrive at the alarmed premises.)

Section 5.
Installation.

The IDS at the facility, area or container shall be installed by a UL listed alarm installing company or by a company approved by the DSO. When connected to a commercial central station, CMS protective signaling service or residential monitoring station, the service provided shall include line security (i.e., the connecting lines are electronically supervised to detect evidence of tampering or malfunction). If line security is not available, then two independent means of transmission of the alarm signal from the alarmed area to the monitoring station must be provided. In all cases, the extent of protection for a container shall be complete.

Section 6.
Certification of Compliance.

Evidence of compliance with the requirements of this Annex will consist of a valid (current) UL Certificate for the appropriate category of service. This certificate will have been issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company: (a) Is listed as furnishing security systems of the category indicated; (b) Is authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by UL for the class; and (c) Is subject to the UL field countercheck program whereby periodic inspections are made of representative alarm installations by UL personnel to verify the correctness of certification practices.

Section 7.
Exceptional Cases

a. If the requirements set forth above cannot be met due to extenuating circumstances, the component may request DSO approval for an alarm system that is:

(1.) Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization.

(2.) Connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the component, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization. Personnel monitoring alarm signals at police stations or dispatch centers do not require PCL's. Police department response systems may be requested only when:

(a.) The component facility is located in an area where central control station services are not available with line security and/or proprietary security force personnel, or a contractually dispatched response to an alarm signal cannot be achieved within the time limits required by the DSO; and I

(b.) It is impractical for the component to establish a proprietary guard force at that location. Nonetheless, installation of these type systems must use UL listed equipment and be accomplished by an alarm installation company that is listed by UL for any of the following categories:

i. Defense (National) Industrial Security Systems;
ii. Proprietary Alarm Systems;
iii. Central Station Burglar Alarm Systems; or
iv. Police Station Connected Burglar Alarm Systems.

b. An installation proposal, explaining how the system would operate, shall be submitted to the DSO. The proposal must include sufficient justification for the granting of an exception and the full name and address of the police department that will monitor the system and provide the required response. The name and address of the UL listed company that will install the system and inspect, maintain, and repair the equipment also shall be furnished.

c. The component shall require a 15-minute response time from the police department. Arrangements shall be made with the police to immediately notify a component representative on receipt of the alarm. The component representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material.

d. In exceptional cases where central station monitoring service is available, but no proprietary security force of central station or subcontracted guard response is available, and where the police department does not agree to respond to alarms, and no other manner of investigative response is available, the DSO may approve cleared employees as the sole means of response.

Annex G
Sanitizing and Releasing Computer Components

Section 1.
General

G-100. Policy. This Annex provides guidance for *sanitization, declassification,* and release of information on *Information Systems storage devices.* Information stored on these devices may range from Unclassified to Top Secret Codeword and may include compartmented, sensitive, or limited-distribution material. This Annex:

a. Provides guidance regarding the known risks and weaknesses associated with sanitizing, and declassifying storage devices and equipment.

b. Indicates what steps may be undertaken to verify that clearing and sanitizing procedures were properly implemented.

c. Provides options for the disposal/destruction of unserviceable storage devices and equipment.

G-101. Procedures. The proliferation of various types of IT storage devices, such as magnetic recording media, optical media, and solid-state semiconductor memory devices, has resulted in the development of separate procedures for clearing and declassification. Guidance for the clearing, sanitization, declassification, and release of IT storage devices not covered by this document may be obtained by submitting all pertinent information to Department Security Officer.

G-102. Terms.

a. Burning - Atendency for an image that is shown on a display over a long period of time to become permanently fixed on the display. This is most often seen in emissive displays such as Cathode Ray Tube (CRT) and Plasma, because chemical changes can occur in the phosphors when exposed repeatedly to the same electrical signals.

b. Coercive Force - A negative or reverse magnetic force applied for the purpose of reducing magnetic flux density.

c. Coercivity - A property of magnetic material, measured in *Oersteds*, used as a measure of the amount of *coercive force* required to reduce the magnetic induction to zero from its remanent state. Generally used as a measure of the difficulty with which magnetic IS storage devices can be degaussed.

d. Declassification - An administrative step that the owner of the storage device takes when the classification is lowered to UNCLASSIFIED. The storage device must be properly sanitized before it can be downgraded to UNCLASSIFIED.

e. Degauss –

(1.) To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force. Commonly referred to as demagnetizing.

(2.) To reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data.

f. Degausser - An electrical device or hand-held permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices or other magnetic material.

g. Degaussing (Demagnetizing) - Procedure using a NSA approved device to reduce the magnetization of a magnetic storage device to zero by applying a reverse (coercive) magnetizing force rendering any previously stored data unreadable and unintelligible.

h. Destruction. Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data.

i. Gauss - A unit of measure of magnetic flux density.

j. Information Technology (IT) Storage Devices - The physical storage devices used by an IS upon which data is recorded.

k. Oersted (Oe)- The unit of measure of a magnetic field.

l. Recycling - End state for IS storage devices processed in such a way as to make them ready for reuse, adapt them to a new use, or to reclaim constituent materials of value.

m. Sanitization - The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. Properly sanitized storage devices may be subsequently declassified upon completion of the organization's respective verification and review procedures.

Section 2.
General Requirements.

G-200. Media Disposal.

a. Media consists of any substance upon which information is recorded by a computer. Disposition procedures for media used to process or store classified or sensitive information must be identified in the security plan.

b. Classified computer system media must be protected and marked in accordance with Chapter 5 and Section 8-205 of this manual and classified media shall be properly protected until declassified or destroyed.

c. Due to the rapidly changing nature of computer media, and threats to the media, the specific method used to purge or destroy media must be approved in writing by the SPM. The SPM, in consultation with the DSO, must consider the most current threats to the specific media when approving destruction methods, which shall meet Department requirements. Specific guidance for the purging, declassification, disposition, or destruction of media is available from the DSO. The general destruction methods are listed below.

(1.) When no longer usable, diskettes, tape cartridges, hard drives, and other media used to process SBU and classified information may be degaussed with the appropriate NSA approved degausser. Consult the current NSA Degausser Products List to determine the appropriate degausser. If degaussing equipment is used, the Information System Security Officer shall establish procedures to ensure strict compliance with the manufacturer's instructions for the operation and continued effectiveness of the equipment.

(2.) Magnetic floppy disks containing classified and sensitive information may also be destroyed by burning or shredding. Crosscut shredders, which meet the requirements set forth in Chapter 6, Section 6-201 and 6-600 may be used to destroy magnetic floppy disks that have been removed from the protective covering.

(3.) The security inspection and release form or similar documentation, attached in Section 4 of this Annex, shall be used to document the release or disposal of any IT system or processing component.

G-201. Media Reuse. When no longer required for mission or project completion, IT storage media that will be re-utilized by another person within the component shall be overwritten with Department CIO approved software or degaussed as appropriate. The media shall be protected consistent with the data sensitivity and/or at the highest classification level at which they were previously used, unless the media has been properly sanitized by using the appropriate NSA approved degausser. The degaussing of hard disks may cause damage (i.e., loss of timing tracks and servo motors), which may prohibit their continued use. The procedures shall be documented in the system security plan.

G-202. Media Release.

a. IT systems that have processed, stored, or transmitted classified information shall not be released from a component's control until the equipment is sanitized.

b. Department IT equipment under maintenance warranty contracts shall include stipulations that equipment removed from the Department's physically protected offices shall be sanitized before its removal.

c. The security inspection and release form or similar documentation, attached in Section 4 of this Annex, shall be used to document the release or disposal of any IT system or processing component.

G-203. Release of Systems and Components. The designated IT security person shall develop equipment removal procedures for systems and components and these procedures shall be stated in the SSAA/SSP. When such equipment is no longer needed, it can be released if:

a. It is inspected by the designated IT security person. This inspection will assure that all media, including internal disks, have been removed or sanitized.

b. A record is created of the equipment release indicating the procedure used for sanitization and to whom the equipment was released. The record of release shall be retained for a period prescribed by the DAA.

c. Procedures specified by the DAA are used.

G-204. Documenting IT System Release or Disposal. The form found in Section 4 of this Annex or similar form/documentation, will be used to document the local release or disposal of any IT system or processing component.

G-205. Intelligence Information. Elements containing intelligence information shall be sanitized in accordance with the policy contained in the Director of Central Intelligence Directive (DCID) 6/3, or successor.

G-206. Malfunctioning Media. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing will be reported to the designated IT security person. The designated IT security person will coordinate the repair or destruction of the media with the responsible DAA. If the hard drive is under a warranty which requires return of the hard drive, dismantle the hard drive and return the case but do not send the platter to the manufacturer.

G-207. Destroying Media. Data storage media will be destroyed in accordance with DAA methods and in accordance with DOJ policy.

G-208. Degausser Requirements. Refer to the current issue of the NSA approved Degausser Products list for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to assure continued compliance with the appropriate specification. National specifications provide a test procedure to verify continued compliance with the specification.

Section 3.
Specific Device Procedures

G-300. Procedures. Guidance for the sanitization, declassification, and release of IS storage devices not covered by this ssection may be obtained by submitting all pertinent information to the DSO.

G-301. Magnetic Storage Devices.

a. Magnetic Tapes

(1.) Sanitization: Sanitize magnetic tapes in accordance with either of the following procedures. Remove all labels or markings that indicate previous use or classification.

(a.) *Degaussing*: Degauss using an NSA evaluated degausser.
(b.) *Incineration*: Incinerate magnetic tape in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials.

(2.) Declassification: Declassify magnetic tapes only after approved verification and review procedures are completed.

(3.) Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified magnetic tapes may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

b. Magnetic Disks: Magnetic disks include hard disk drives and diskettes.

(1.) Hard Disk Drives
(a.) *Sanitization:* Sanitize hard disk drives using one of the following procedures. Remove all labels or markings that indicate previous use or classification.
i. Sanitization with Automatic Degausser: (1) Remove the hard disk drive from the chassis or cabinet; (2) remove any steel shielding materials or mounting brackets which may interfere with magnetic fields; (3) place the hard disk drive in an NSA approved degausser and erase. Although not required, it is highly recommended that the hard disk drive be physically damaged prior to release. NOTE – ERASURE OF HARD DISK DRIVES CAUSES PERMANENT DAMAGE THAT PROHIBITS THEIR CONTINUED USE.
i. Sanitization with Degaussing Wand: Sanitize hard disk drives by disassembling the device and erasing all surfaces of the enclosed platters with an NSA/CSS evaluated handheld degaussing wand. Although not required, it is highly recommended that the hard disk drive be physically damaged prior to release. *NOTE – ERASURE OF HARD DISK DRIVES CAUSES PERMANENT DAMAGE THAT PROHIBITS THEIR CONTINUED USE.*
ii. Sanitization by Incineration: Incinerate hard disk drives in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials.
(b.) *Declassification*: Declassify hard disk drives only after approved verification and review procedures are completed.
(c.) *Release*: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified hard disk drives may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

(2.) Diskettes
(a.) *Sanitization:* Sanitize diskettes by degaussing, shredding, or incineration. Remove all labels or markings that indicate previous use or classification.
i. Sanitization by Degaussing: Degauss the diskettes in an NSA evaluated degausser.
ii. Sanitization by Shredding: Shred diskettes using an approved high security crosscut paper shredder. Remove diskette cover and metal hub prior to shredding.
iii. Sanitization by Disintegration: Disintegrate diskettes using an approved high security disintegrator.
iv. Sanitization by Incineration: Incinerate diskettes in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials.
(b.) *Declassification*: Declassify diskettes only after approved verification and review procedures are completed.
(c.) *Release*: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified diskettes may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

G-302. Optical Storage Devices. Optical storage devices include Compact Disks (CD) and Digital Versatile Disks(DVD)

a. Sanitization: Sanitize optical storage devices using one of the following procedures. Remove all labels or markings that indicate previous use or classification.

(3.) Sanitization by Grinding: Use an approved optical storage device grinder, to remove the information bearing layers of only CD storage devices. DVD's cannot be sanitized by this method since the information bearing layers are sandwiched in the center.

(4.) Sanitization by Shredder or Disintegrator: Use an approved optical storage device shredder, or disintegrator, to reduce CD and DVD storage devices into particles that have nominal edge dimensions of 5 millimeters or less and surface area of 25 square millimeters or less.

(5.) Sanitization by Embossing/Knurling: Use an approved optical storage device embosser/knurler, for CD and DVD storage devices.

(6.) Sanitization by Incineration: Incinerate optical storage devices in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials. Material must be reduced to white ash.

b. Declassification: Declassify optical storage devices only after approved verification and review procedures are completed.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified optical storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

G-303. Solid State Storage Devices. Solid State Storage Devices include Random Access Memory (RAM), Read Only Memory (ROM), Field Programmable Gate Array (FPGA), Smart Cards, and Flash Memory.

a. Sanitization: Sanitize solidstate devices with the following procedures or sanitize by smelting in a licensed furnace at 1,600 degrees Celsius or higher or disintegrate into particles that are nominally 2 millimeter edge length in size using an approved disintegrator. Remove all labels or markings that indicate previous use or classification.

(1.) DRAM and SRAM: Sanitize DRAM and SRAM by removing the power. Once power is removed, sanitization is instantaneous. Or, sanitize functioning DRAM and SRAM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly rereading the overwritten information to confirm that only the known pattern can be recovered.

(2.) Ferroelectric Random Access Memory (FRAM) and Magnetic Random Access Memory (MRAM) (NonVolatile): Sanitize functioning FRAM and MRAM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly rereading the overwritten information to confirm that only the known pattern can be recovered.

(3.) EPROM and UVEPROM: Sanitize EPROM and UVEPROM by performing an ultraviolet erase according to the manufacturer's recommendations,but increase the time requirement by a factor of three. Next, overwrite all bit locations with a known unclassified pattern.

(4.) EEPROM: Sanitize EEPROM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly rereading the overwritten information to confirm that only the known pattern can be recovered.

(5.) PROM: Sanitize only by smelting.

(6.) FPGA (NonVolatile): Sanitize FPGA by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly rereading the overwritten information to confirm that only the known pattern can be recovered.

(7.) FPGA (Volatile): Sanitize FPGA by removing the power. Once power is removed, sanitization is instantaneous.

(8.) Smart Cards: Sanitize Smart Cards by shredding with a strip shredder or with scissors.

(a.) Sanitization with a Strip Shredder: A strip shredder with a maximum width of 2 millimeters will destroy the microchip, barcode, magnetic strip and written information on the Smart Card. Smart Cards must be inserted diagonally into the strip shredder at a 45degree angle for proper sanitization. NOTE: A CROSS CUT SHREDDER WILL NOT SANITIZE SMART CARDS.

(b.) Sanitization with Scissors: Cut the Smart Card into strips diagonally at a 45degree angle, insuring that the microchip is cut through the center. Insure that the barcode, magnetic strip, and written information are cut into several pieces and the written information is unreadable.

(9.) Flash Memory: Sanitize EEPROM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly rereading the overwritten information to confirm that only the known pattern can be recovered.

b. Declassification: Declassify solidstate storage devices only after approved verification and review procedures are completed.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified solidstate storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

G-304. Hard Copy Storage Devices. Hard Copy Storage Devices include paper, microforms, and monitors with burnin.

a. Sanitization: Sanitize hard copy storage devices with the following procedures.

(1.) Sanitize paper by burning, chopping, crosscut shredding using an approved crosscut shredder, pulverizing, or wet pulping. When burned, material residue must be reduced to white ash. When chopping, shredding, pulverizing, or wet pulping, material residue must be reduced to pieces 5 millimeters square or smaller.

(2.) Sanitize microforms (microfilm, microfiche, or other reduced image photo negatives) by burning or by chemical means, such as immersion in household bleach (i.e., sodium hypochlorite) for film masters and acetone or methylene chloride for diazo

reproductions. When burned, material residue must be reduced to white ash.

(3.) Sanitize monitors exhibiting burning by destroying the surface of the monitor into pieces no larger than 5 centimeters square.

b. Declassification: Declassify hard copy storage devices only after approved verification and review procedures are completed.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified hard copy storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

Section 4.
Security Inspection and Release Form

(Form found on next page)

SECURITY CLASSIFICATION

SECURITY INSPECTION AND RELEASE AUTHORITY

INSTRUCTIONS

Complete Part 1 of this form to document the local release or disposal of any component *(for example, printer)* or subcomponent *(for example, printed circuit board)* being removed from any Information Technology (IT) system. File copy of the completed form with the accreditation package. Forward the original forms to the Information Systems Security Manager (ISSM) if used to document an entire IT system for which the accreditation package has to be formally rescinded and components formally released.

PART 1.
TO BE COMPLETED BY THE ISSO OR EQUIPMENT CUSTODIAN

1. TYPE OR PRINT NAME AND TITLE	2. GRADE	3. DATE

4. ORGANIZATION OFFICE SYMBOL. RETURN MAILING ADDRESS	5. OFFICE PHONE NUMBER

		YES	NO
6. EQUIPMENT PROCESSED CLASSIFIED INFORMATION?			
7. EQUIPMENT CONTAINS ELECTRONIC OR MAGNETIC STORAGE CAPABILITY?			
8.	EQUIPMENT PHYSICALLY SEARCHED FOR CLASSIFIED MATERIAL?		
	IF CLASSIFIED EQUIPMENT WAS FOUND, WAS A SECURITY INVESTIGATION INITIATED?		
9.	EQUIPMENT DEGAUSSED?		
	If YES provide the name, model, and date of last calibration of the degausser		
10. EQUIPMENT OVERWRITTEN? (If YES, attach description of the override procedure)			

11. ACCREDITATION PACKAGE NUMBER	12. REASON FOR RELEASE

13. ENTER ALL ITEMS TO BE RELEASED

MODEL	DESCRIPTION	SERIAL	SERIAL *(Identify declassification)*		
			DESTROY	DEGAUSS	OVER WRITE

14. COMMENTS

15. SIGNATURE OF INDIVIDUAL IN PART 1	16. DATE
17. ISSO SIGNATURE	18. DATE

PART II.
TO BE COMPLETED BY THE ISSM ONCE SIGNED BY THE DAA, THE ACCREDITATION OF THIS IS (ITEM 11) IS HEREBY RESCINDED AND THE EQUIPMENT (ITEM 13) IS AUTHORIZED FOR RELEASE/ DISPOSAL

19. ISSM SIGNATURE	19. DATE
20. DAA SIGNATURE	21. DATE

Annex H
Safeguarding Classified Information on Laptop/Notebook Computers

Section 1.
Introduction

Prior to processing classified information, laptop/notebook computers or any other computers designed to allow periodic relocation must be accredited in accordance with DOJ Order 2640.2F and standards developed by the Department CIO.

a. The accreditation document will indicate exactly where the computer may be taken and the classification level of the information that may be processed on the computer. Accreditation for laptop or notebook computers generally must address processing in the user's normal work location and in the off-site location.

b. Classified processing may be done on laptop or notebook computers if it occurs in normal work areas otherwise acceptable for the storage, preparation, or discussion of classified material. The accrediting authority may limit the classified processing to the user's regular place of work or, in cases of compelling operational need, may include approved areas while at a travel location. Classified information SHALL ONLY be processed at U.S. Government facilities or approved U.S. Government contractor facilities (see Section 8-211 of this manual). Media or output products, including marking and storage standards, must be handled in accordance with chapter 5 and 6 of this manual.

c. If the computer configuration includes non-removable hard disks that store classified material, the entire system must be stored in an area approved for storage of the highest classification of information the system is accredited to process when left unattended.

Section 2.
Transporting Laptops in and out of a SCIF.

Laptops or other portable computers, regardless of the classification of the data processed, will not be allowed in and out of a Sensitive Compartmented Information Facility (SCIF) and should not be procured/obtained for that environment. When the operational mission requires automation support for an individual on official travel, prior arrangements should be made with the site(s) he/she is visiting for the required automation support. For collateral information processing, arrangements should be made to use laptops outside the SCIF(s). For Sensitive Compartmented Information (SCI) processing, arrangements should be made to use compatible IT systems processing capability available at the visited SCIF(s) so that only software/data is transported. Exceptions to this policy will be granted by the SCIF Control Officer (SCO) on a case-by-case basis under the following criteria:

a. Approval must be obtained prior to movement of the computer.

b. The approval request must include the date of the IT system accreditation and accreditation official for the computer(s) involved.

c. Laptops with built-in modems are not authorized to be connected to any circuit within a SCIF. Laptops without built-in modems will not be connected to a modem while in a SCIF.

d. Program and/or data disks associated with the laptop must be labeled with the highest classification of the data contained therein, including the unclassified label when applicable. A diskette brought into a SCIF will not be taken out unless the SCO or his/her designee has verified that the label properly reflects the diskette's classification. Storage media containing software programs and/or data files and information will, regardless of source of ownership, not be removed from a SCIF without the prior coordination and approval of the user's supervisor, and SCO.

Section 3.
Traveling with Classified Laptops

When traveling with classified laptops, cleared couriers must ensure both laptop and disks are prepared according to Chapter 5 and 6 of this manual. In addition:

a. Laptops must meet the requirements identified in DOJ Order 2640.2F and the IT Security Standards issued by the Department CIO.

b. Laptops shall have an outer container when the classified data is stored in the internal memory or maintained on fixed storage media.

c. Laptops and storage media containing classified information shall be kept under constant surveillance or stored in secure containers/facilities.

d. If you are traveling via commercial air with classified materials, especially a laptop computer, you should advise the Transportation Security Administration (TSA) in advance by calling the TSA office at the airport from which you'll be departing. The TSA office will notify the appropriate officials at the airport. For airport TSA offices please check the local phone directory . You will be screened like any other passenger, and the screener may use explosive trace detection swabs on the outer laptop wrapping. If the results are positive, the TSA officials will x-ray the wrapped laptop. There should be no need to open and turn on the laptop.

Annex I
Reproduction on Digital Equipment

Section 1.
Introduction

This Annex provides the policy for making digital copies for classified and unclassified reproduction either in a standalone or networked configuration. These devices are computer driven and therefore constitute an Information Technology (IT) system subject to many of the same security vulnerabilities as any other computer devices. This policy applies not only to digital copiers, but also to peripheral equipment with multi-function capabilities to copy, print, scan, fax, and store sensitive/classified information and this type of equipment will be referred to as digital copiers though out this Annex.

Section 2.
Digital Copiers

Computer based, network capable devices with processors, memory, hard drives, image retention components, and in some cases, wireless connections and cellular phone transmitters with vendor auto alert features.

Section 3.
Policy

a. Digital copiers used for classified reproduction shall not be connected to an unclassified network.

b. Networked digital copiers are only permitted to process information to the accredited classification level of the network itself.

c. Digital copiers connected to a classified network shall be approved by the Component's Security Program Manager and the Designated Accreditation Authority for the network.

d. When connected to a network, digital copiers will assume the highest classification for which the network is accredited and, if also operated as a standalone device, they will assume the highest classification of copied documents. It should be kept in mind when using digital copier equipment that the document image will remain on the imaging surface, hard drives, and static RAM.

e. All digital copiers used strictly for unclassified purposes may not be connected to a classified network and must be clearly marked for unclassified use only. This is intended to preclude anyone from inadvertently using them to copy (and incidentally store) classified information.

f. Reproduction of classified information shall also be accomplished in accordance with Chapter 6-105 of this manual.

g. Digital copiers used for classified processing may not be directly connected to telephone lines. Remote maintenance or programming will not be permitted on these devices. Exceptions may be granted on a case by case basis. Exceptions may be granted if all data storage components or other internal memory components contained in the system are properly cleared and verified prior to the remote maintenance or programming.

h. Components shall not lease digital copiers to process classified information. Exceptions to this policy can only be granted by the Department Security Officer on a case by case basis. Exceptions may be granted if the programmable circuit boards, data storage components, or other internal memory components contained in the system are the property of the Department.

i. All maintenance of copiers used for classified reproduction must be performed on site, either by cleared personnel or by commercial technicians under escort by component personnel. Any parts removed or replaced during maintenance, particularly programmable circuit boards or data storage components, must by retained by the Component for secure disposal. If Portable Electronic Devices (PEDs) are required for diagnostics, they must be purchased (software included) and maintained in appropriate secure facilities.

j. Digital copiers used for classified reproduction in areas not approved for the open storage of classified information may only be used if approved in writing by the Department Security Officer (DSO). Digital copier products approved by the National Information Assurance Partnership (NIAP) shall be used in the aforementioned operating environment. A listing of evaluated products can be viewed via the internet at http://www.commoncriteriaportal.org/http://www.niap.nist.gov (Select certified products and then other devices) Consideration should also be given to these products for use on digital copiers regardless of the classification of the information and area where reproduction is being performed especially if they contain National Security Information (NSI) or Personally Identifiable Information (PII). Digital copiers used for classified reproduction which have NIAP approved overwrite kits shall not be connected to an unclassified network.

k. All digital copiers reproducing Sensitive Compartmented Information (SCI) shall be located in an approved Sensitive Compartmented Information Facility (SCIF).

Section 4.
Procedures for Classified Digital Copiers

a. Since these copiers have internal electronic memory components, it is necessary to purchase them outright (not lease them unless an exception is granted as outlined in paragraph L-102h above). All electronic parts that contain

a memory/data eminence capacity must be maintained under absolute control and have a maintenance contract that provides for maintenance support by cleared personnel.

b. Removal /return of purely mechanical or electro-mechanical parts to a vendor will only be permitted based on a risk determination that includes consideration of threat, vulnerability, impact, and cost.

c. Printed circuit boards, memory boards with possible classified information stored on them are to be destroyed as classified components. The only exception permitted is if a part can be absolutely cleansed in accordance with the media sanitization and release policies and procedures identified in appendix G of this manual.

d. All communications ports not specifically required for networked or contractual maintenance must be removed or permanently disabled. Only hardwired connections are permitted (no IR, RF, or Audio communications). This provision must be included in the purchase contract.

e. If PEDs are required for diagnostics, they must be purchased (software included) and maintained in appropriate secure facilities.

Section 5.
Procedures for Unclassified Digital Copiers

a. If unclassified NSI or PII has been reproduced on a digital copier it must be controlled in the same manor as a digital copiers that reproduced classified information. (Ref. L-103)

b. All other digital copiers used for unclassified reproduction must be controlled IAW Chapter 8 of this document.

Annex J
References

Atomic Energy Act of 1954, as amended
CNSS Policy No. 300 – "National Policy on Control of Compromising Emanations"
CNSS Instruction 4005 – "Safeguarding Communications Security (COMSEC) Facilities and Material"
DOJ Order 2600.2C – "Security Programs and Responsibilities", or its successor
DOJ Order 2610.2A – "Employment Security Regulations"
DOJ Order 2640.2F – "Information Technology Security"
DOJ Classification Guide
DOJ COMSEC Manual
DOJ's Incident Response Procedures for Data Breaches Involving Personally Identifiable Information
Executive Order 12968, as amended – "Access to Classified Information"
Executive Order 12829, as amended – "National Industrial Security Program"
Executive Order 12333, as amended – "United States Intelligence Activities"
Executive Order 13526 – "Classified National Security Information"
Executive Order 13556 – "Controlled Unclassified Information (CUI)"
Federal Specification FF-P-110
Federal Standard 809
Federal Standard 832
Intelligence Community Directive (ICD) 503
ISOO Implementing Directive 1
NIAP Assurance Maintenance Program
National Industrial Security Program
National Industrial Security Program Operating Manual
National Security Telecommunications and Information Systems Security Policy Number 11
NTISSI No. 7000 – "TEMPEST Countermeasures for Facilities"
10 CFR Part 1045
28 CFR Part 17 – "Classified National Security Information and Access to Classified Information"
28 CFR Part 17 § 17.15
32 CFR Part 2001 – "the Directive"
39 CFR
5 U.S.C. 552 - Freedom of Information Act
5 U.S.C. 552a – Privacy Act of 1974
12 U.S.C. 3401
15 U.S.C. 1681 – Fair Credit Reporting Act
31 U.S.C. 5312
31 U.S.C. 9701
42 U.S.C. 2162(e)
50 U.S.C. 403
50 U.S.C. 421 - Intelligence Identities Protection Act of 1982
DD Form 254 – "Contract Security Classification Specification"
DOJ Form 504 – "Notification of Foreign Travel"
DOJ Form 555 – "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
Standard Form 311 – "Agency Security Classification Management Program Data"
Standard Form 312 – "Classified Information Nondisclosure Agreement"
Standard Form 700 – "Security Container Information"
Standard Form 701 – "Activity Security Checklist"
Standard Form 702 – "Security Container Checksheet"
Standard Form 713 – "Consent for Access to Records"
Standard Form 85 – "Questionnaire for Non-Sensitive Positions"
Standard Form 85P – "Questionnaire for Public Trust Positions"
Standard Form 86 – "Questionnaire for National Security Positions"
Standard Form 86A – "Continuation Sheet for SF86, SF85, and SF85-P"
Standard Form 86C – "Standard Form 86 Certification"