

National Security Information Handbook

December 2006

Revision 1



This page is intentionally blank



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

February 1, 2005

OFFICE OF
ADMINISTRATION
AND RESOURCES
MANAGEMENT

This handbook is issued under the authority of Executive Order 12958, "Classified National Security Information", as amended, March 28, 2003. I have approved it for publication in my capacity as EPA's designated Senior Agency Official for National Security Information (NSI). The handbook sets forth EPA's procedures for the proper handling and maintenance of NSI and is effective immediately.

Copies of this handbook may be obtained from the Office of Administration and Resources Management (OARM) NSI Program Team and are available on the Agency Intranet at http://dcwww.dcicc.epa.gov:9876/oa/HQ_sec/.

A handwritten signature in cursive script that reads "David J. O'Connor".

David J. O'Connor
Acting Assistant Administrator
Office of Administration and Resources Management

Internet Address (URL) • <http://www.epa.gov>

Recycled/Recyclable • Printed with Vegetable Oil Based Inks on Recycled Paper (Minimum 30% Postconsumer)

This page is intentionally blank

TABLE OF CONTENTS

TABLE OF CONTENTS	V
GLOSSARY OF ACRONYMS AND ABBREVIATIONS.....	XIII
CHAPTER 1: POLICY AND PROGRAM MANAGEMENT	1-1
Section 1: General.....	1-1
1-100 Overview.....	1-1
1-101 Authority.....	1-1
1-102 Definitions.....	1-1
1-103 Policies.....	1-1
Section 2: NSI Program Management	1-2
1-200 Roles and Responsibilities	1-2
Section 3: Preliminary Inquiries and Investigations	1-3
1-300 Reporting Requirement.....	1-3
1-301 Incident Reporting Procedures.....	1-4
Section 4: Administrative Sanctions.....	1-5
1-400 Federal and Non-Federal Employee Administrative Sanction Requirements .	1-5
Section 5: Reports	1-5
1-500 Reporting Requirements	1-5
Section 6: Self-Inspection, Program Assessments, and Inspections.....	1-5
1-600 Requirements	1-5
1-601 Self-Inspections.....	1-5
1-602 Assessment Visits	1-6
1-603 Inspections	1-6
Section 7: Emergency Release of Classified Information.....	1-6
1-700 Emergency Release of Classified Information	1-6
CHAPTER 2: SECURITY CLASSIFICATION.....	2-1
Section 1: Overview	2-1
2-100 Overview.....	2-1
Section 2: Original Classification	2-1
2-200 Classification Principles.....	2-1
2-201 Classification Standards.....	2-1

2-202	Classification Levels.....	2-1
2-203	Original Classification Authority.....	2-2
2-204	Classification Categories	2-3
2-205	Limitations and Prohibitions.....	2-3
2-206	Documents Proposed for Original Classification Decisions.....	2-3
2-207	Duration of Classification.....	2-4
2-208	Security Classification/Declassification Guides.....	2-4
2-209	Reclassification of Information.....	2-5
2-210	Downgrading Classified Information	2-6
2-211	Classification Challenges.....	2-6
Section 3: Derivative Classification.....		2-8
2-300	Derivative Classification Principles.....	2-8
2-301	Derivative Classification Procedures.....	2-8
CHAPTER 3: DECLASSIFICATION.....		3-1
Section 1: Overview		3-1
3-100	Overview.....	3-1
Section 2: General.....		3-1
3-200	Requirement.....	3-1
Section 3: Declassification Systems		3-2
3-300	Automatic Declassification.....	3-2
3-301	Systematic Declassification Review	3-3
3-302	Mandatory Declassification Review	3-3
CHAPTER 4: IDENTIFICATION AND MARKING.....		4-1
Section 1: Overview		4-1
4-100	Overview.....	4-1
Section 2: General.....		4-1
4-200	Requirements	4-1
4-201	Marking Standards.....	4-1
Section 3: Original Classification Markings.....		4-2
4-300	Required Original Classification Markings	4-2
4-301	Marking Examples for Originally Classified Information.....	4-2
Section 4: Derivative Classification Markings		4-3
4-400	Required Derivative Classification Markings.....	4-3
4-401	Marking Examples for Derivative Classification	4-4
Section 5: Additional Marking Requirements		4-5
4-500	Marking Prohibitions	4-5

4-501	Documents Proposed for Original Classification	4-5
4-502	Transmittal Documents	4-6
4-503	Files, Folders, and Binders.....	4-6
4-504	Classified Working Papers.....	4-6
4-505	Charts, Maps, Graphs, and Drawings	4-6
4-506	Photographs, Films, and Recordings	4-7
4-507	Information Used for Training Purposes	4-7
4-508	Automated Information Technology (IT) Storage Media.....	4-7
4-509	Classified Documents Produced by Classified Information Systems.....	4-8
Section 6: Declassification Markings		4-8
4-600	General.....	4-8
4-601	Procedures.....	4-8
CHAPTER 5: SAFEGUARDING.....		5-1
Section 1: Overview		5-1
5-100	Overview.....	5-1
Section 2: General.....		5-1
5-200	Requirements	5-1
Section 3: Access		5-1
5-300	General Restrictions on Access	5-1
Section 4: Document Accountability and Review		5-2
5-400	Policy	5-2
5-401	Top Secret Document Accountability.....	5-2
5-402	Secret and Confidential Document Review	5-2
5-403	Return of Classified Information	5-3
Section 5: Storage.....		5-3
5-500	Policy	5-3
5-501	Storage Standards.....	5-3
5-502	Storage of Classified Information.....	5-4
5-503	Combinations	5-4
5-504	End of Day Checks	5-5
5-505	Security Container Check Sheet and Open/Closed Signs.....	5-5
Section 6: Types of Secure Areas.....		5-5
5-600	Principles and Concepts	5-5
5-601	Accreditation Procedures	5-6
5-602	Open Storage Accredited Area	5-7
5-603	Secure Accredited Area	5-9
5-604	Restricted Area.....	5-10
Section 7: Reproduction of Classified Information		5-10

5-700	General.....	5-10
5-701	Requirements	5-10
5-702	Procedures.....	5-11
Section 8: Destruction.....		5-12
5-800	Policy	5-12
5-801	Authorized Destruction Methods.....	5-12
5-802	Unauthorized Destruction Methods	5-12
CHAPTER 6: TRANSMISSION METHODS.....		6-1
Section 1: Overview		6-1
6-100	Overview.....	6-1
Section 2: General.....		6-1
6-200	Requirements	6-1
Section 3: Packaging for Transmission.....		6-2
6-300	Packaging Requirements for Mailing and Couriering outside EPA	6-2
Section 4: Methods of Transmission		6-2
6-400	Top Secret Information	6-2
6-401	Secret Information	6-2
6-402	Confidential Information	6-3
6-403	Transmissions to a U.S. Government Facility Located Outside the U.S.....	6-3
Section 5: Hand-Carrying Classified Information		6-3
6-500	General Policy.....	6-3
6-501	Courier Cards.....	6-4
6-502	Courier Requirements and Responsibilities.....	6-4
6-503	Hand-Carry Authorization for Out of Area or Aircraft Travel.....	6-5
6-504	Authorization to Hand-Carry Information to an Overseas Location	6-6
CHAPTER 7: SECURITY EDUCATION AND TRAINING.....		7-1
Section 1: Overview		7-1
7-100	Overview.....	7-1
Section 2: General.....		7-1
7-200	Roles and Responsibilities	7-1
Section 3: Initial Orientation Training		7-1
7-300	Initial Orientation.....	7-1
Section 4: Specialized Security Training		7-2
7-400	General.....	7-2
7-401	Original Classification Authorities	7-2

7-402	NSI Representatives.....	7-2
7-403	Courier Training.....	7-3
7-404	Other Types of Training.....	7-3
Section 5: Annual Refresher Security Training.....		7-3
7-500	Annual Refresher Training	7-3
Section 6: Termination Briefings.....		7-3
7-600	Termination Briefings.....	7-3
CHAPTER 8: FOREIGN GOVERNMENT INFORMATION.....		8-1
Section 1: Overview		8-1
8-100	Overview.....	8-1
Section 2: Protection of Foreign Government Information.....		8-1
8-200	General.....	8-1
8-201	Requirements for Safeguarding Foreign Government Information.....	8-1
8-202	Safeguarding Foreign Government Information.....	8-1
8-203	Transmission Methods.....	8-3
8-204	Marking Foreign Government Information	8-3
8-205	Declassification of Foreign Government Information.....	8-3
8-206	Third Party Release.....	8-3
CHAPTER 9: INDUSTRIAL SECURITY		9-1
Section 1: General.....		9-1
9-100	Overview.....	9-1
9-101	Authority	9-1
9-102	Policy	9-1
Section 2: Program Management.....		9-2
9-200	Roles and Responsibilities	9-2
Section 3: Requirements.....		9-3
9-300	General.....	9-3
9-301	Security Requirement Contract Clause.....	9-3
9-302	Contract Security Classification Specification (DD 254).....	9-3
9-303	Contractor Eligibility Requirements	9-4
Section 4: Visits and Meetings		9-5
9-400	Visits and Meetings.....	9-5
CHAPTER 10: NATIONAL SECURITY SYSTEMS PROGRAM.....		10-1
Section 1: General.....		10-1

10-100	Overview.....	10-1
10-101	Authority.....	10-1
10-102	Policy.....	10-1
10-103	Security Incident Reporting.....	10-1
Section 2: Program Management.....		10-2
10-200	Roles and Responsibilities.....	10-2
Section 3: National Security Systems Identification and Planning.....		10-5
10-300	Identifying Information Systems as National Security Systems.....	10-5
10-301	Classified Information Security Planning Standards.....	10-6
Section 4: Training.....		10-6
10-400	Security Training Requirements.....	10-6
Section 5: Classified Processing Standards.....		10-7
10-500	Personnel Security.....	10-7
10-501	Physical Security.....	10-8
10-502	Administrative Security.....	10-9
10-503	Technical Security.....	10-13
CHAPTER 11: SPECIAL ACCESS PROGRAMS.....		11-1
Section 1: Overview.....		11-1
11-100	Overview.....	11-1
Section 2: Special Access Programs.....		11-1
11-200	Policy.....	11-1
Section 3: Sensitive Compartmented Information (SCI) Program.....		11-1
11-300	Authority.....	11-1
11-301	SCI Program Management.....	11-2
11-302	SCI Administration.....	11-3
11-303	Infractions, Violations, Compromises, and Unauthorized Disclosures.....	11-5
11-304	SCI Facilities (SCIF).....	11-5
11-305	Contracts Requiring SCI Access.....	11-7
11-306	SCI Security Education.....	11-7
11-307	Technical Requirements.....	11-8
APPENDIX A DEFINITIONS.....		A-1
APPENDIX B PRELIMINARY INQUIRY REPORT.....		B-1
APPENDIX C ANNUAL NSI DATA COLLECTION REPORT.....		C-1

APPENDIX D SELF-INSPECTION CHECKLIST D-1

APPENDIX E SAMPLES OF STANDARD FORMSE-1

APPENDIX F ROOM ACCREDITATION CHECKLIST.....F-1

APPENDIX G ACCREDITATION STATUS FORM..... G-1

APPENDIX H CLASSIFIED INFO ACCOUNT RECORD H-1

APPENDIX I COURIER DOCUMENTATION.....I-1

APPENDIX J FGI CLASSIFICATION MATRIX..... J-1

APPENDIX K SECURITY FEATURE DESCRIPTIONS K-1

APPENDIX L SCI AUTHORIZATION REQUEST FORM.....L-1

APPENDIX M SCI VISIT CERTIFICATION REQUEST FORM..... M-1

This page is intentionally blank

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AA	Assistant Administrator
AO	Office of the Administrator, EPA
C	Confidential
CD	Compact Disk
CIA	Central Intelligence Agency
CNSS	Committee on National Security Systems
CO	Contracting Officer
CONOPS	Concept of Operations
COR	Contractor Officer Representative
CSIRC	Computer Security Incident Response Capability
CSS	Central Security Service
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Directive
DCS	Defense Courier Service
DD	Department of Defense
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DSS	Defense Security Services
E.O.	Executive Order
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FCL	Facility Clearance
FGI	Foreign Government Information
FISMA	Federal Information Security Management Act
FOCI	Foreign Ownership Control or Influence
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Facility Security Officer
GSA	General Services Administration
HQ	Headquarters
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identification
IDS	Intrusion Detection System
IRM	Information Resources Manual
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
ISSR	Information System Security Representative
IT	Information Technology
JFAN	Joint Air Force, Army, and Navy
JPAS	Joint Personnel Adjudication System
MOA	Memorandum of Agreement
NARA	National Archives and Records Administration

NATO	North Atlantic Treaty Organization
NFIB	National Foreign Intelligence Board
NIACAP	National Information Assurance Certification and Accreditation Process
NIB	National Intelligence Board
NIP	National Intelligence Program
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security System
NSSP	National Security Systems Program
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OADR	Originating Agency Determination Required
OARM	Office of Administration and Resources Management
OAS	Office of Administrative Services
OCA	Original Classification Authority
OMB	Office of Management and Budget
OSWER	Office of Solid Waste and Emergency Response
PCL	Personnel Security Clearance
PI	Preliminary Inquiry
PIN	Personal Identification Number
PL	Protection Level
ROM	Read-only Memory
S	Secret
SAO	Senior Agency Official
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SMD	Security Management Division
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SSAA	System Security Authorization Agreement
SSO	Special Security Officer
SSP	System Security Plans
TS	Top Secret
U	Unclassified
U.S.C.	United States Code
UK	United Kingdom
VAL	Visit Authorization Letter

Chapter 1: POLICY AND PROGRAM MANAGEMENT

Section 1: General

1-100 Overview

This handbook sets forth the official policies, standards, and procedures for Environmental Protection Agency (EPA) employees and non-federal personnel who have access to classified National Security Information (NSI).

1-101 Authority

The contents of this handbook are derived from the following:

- EPA Order 4850, National Security Information, dated July 28, 2004
- EPA Delegation 1-6-A, National Security Information, dated July 28, 2004
- Executive Order (E.O.) 12958, as amended, "Classified National Security Information", dated March 28, 2003; hereinafter referred to as E.O. 12958
- Information Security Oversight Office (ISOO) directive "Classified National Security Information (Directive No. 1)", Final Rule, dated September 22, 2003; hereinafter referred to as ISOO Dir. No. 1
- Executive Order (E.O.) 12829, as amended, "National Industrial Security Program", dated January 8, 1993; hereinafter referred to as E.O. 12829
- DoD 5522.22-M, National Industrial Security Program Operating Manual, dated February 2006

1-102 Definitions

Definitions for this handbook are provided in Appendix A.

1-103 Policies

1. All employees and non-federal personnel are responsible for protecting classified information under their custody and control. All managers have specific, non-delegable responsibilities for the implementation and management of the NSI Program within their areas of responsibility.
2. Management of classified information shall be included as a critical element or item in the EPA performance plans to be evaluated in the rating of original classification authorities, security managers, NSI Representatives, and other personnel whose duties involve the creation or regular handling of classified information.
3. Employees and non-federal personnel shall have access to classified information only if they possess a valid and appropriate security clearance, have signed a Standard Form (SF) 312, "Classified Information Non-disclosure Agreement," and a valid need-to-know for access to the information.

Section 2: NSI Program Management

1-200 Roles and Responsibilities

The effectiveness of EPA's NSI Program depends on the cooperation and support of all levels of management. This section describes management responsibilities.

1. The Administrator, EPA shall:
 - Commit necessary resources for the effective implementation of the NSI Program
 - Ensure the safeguarding of classified information
 - Designate a Senior Agency Official (SAO) to direct and administer the NSI Program
 - Serve as EPA's Original Classification Authority (OCA)
 - Delegate OCA, when appropriate
2. The Assistant Administrator, Office of Administration & Resources Management (OARM) shall:
 - Serve as SAO to oversee direction and management of the NSI Program
 - Oversee policy development for the NSI Program
 - Establish a security education and training program
 - Establish an Agency-wide self-inspection program, which shall include the periodic review and assessment of the security infrastructure and classified holdings
 - Ensure EPA employees' performance ratings include evaluation for the management of classified infrastructure and holdings
 - Account for the cost associated with the implementation of the NSI Program
 - Ensure compliance with federal mandates
 - Directly communicate with the Information Security Oversight Office (ISOO), on NSI matters
3. The Director, Office of Administrative Services (OAS) shall:
 - Provide guidance and direction on management of the NSI Program
 - Ensure Agency-wide compliance with NSI policies and procedures
4. The Director, Security Management Division (Director, SMD) shall:
 - Administer all matters related to the NSI Program
 - Approve NSI policies and procedures
 - Oversee self-inspections, education and training, outreach, and compliance initiatives
5. The OARM's NSI Program Team, hereinafter referred to as the NSI Program Team shall:
 - Develop NSI Program policies and procedures
 - Develop and maintain an NSI education and training program
 - Develop and implement the self-inspection program

- Maintain all original classification decisions made by the OCA, and the master EPA security classification guide(s)
 - Review Preliminary Inquiry (PI) reports
 - Provide support and oversight of all aspects of Program and Regional NSI Programs
6. The NSI Representative shall:
- At a minimum, hold and maintain a Secret security clearance
 - Serve as the advisor and local point of contact for NSI security related-matters throughout his/her area of responsibility
 - Implement and manage the provisions of this handbook within his/her area of responsibility
 - Develop standard operating procedures (SOPs) tailored to the NSI Handbook
 - Implement local NSI security training and awareness program to ensure personnel are aware of his/her responsibilities
 - Conduct an annual self-inspection of his/her area of responsibility
 - Disseminate new NSI Program requirements to all pertinent employees
 - Ensure that rooms containing NSI are provided the security measures necessary to deter unauthorized persons from gaining access to classified information; specifically, security measures preventing unauthorized visual and/or auditory access
 - Coordinate NSI Program requirements and SOPs with the NSI Program Team
 - Manage classified visit procedures within his/her area of responsibility
 - Complete and forward, to the NSI Program Team, all reporting requirements each fiscal year
 - Ensure accountability records are maintained

Section 3: Preliminary Inquiries and Investigations

1-300 Reporting Requirement

1. Reporting ensures incidents are properly investigated; the necessary actions are taken to negate or minimize the adverse effects of the infraction or violation, and to preclude reoccurrence.
2. The actual or possible loss or compromise of classified information presents a threat to national security and must be reported to an immediate supervisor, NSI Representative, or the NSI Program Team.
 - Loss: occurs when it cannot be physically accounted for or located
 - Compromise: occurs when classified information is disclosed to an unauthorized person(s) who does not have a security clearance, is not authorized access, or does not have a valid need-to-know
3. A successful security management system incorporates many facets of information security including the possible occurrences of violations and infractions.

- Security Violation: Any knowing, willful, or negligent action that:
 - Could reasonably be expected to result in unauthorized disclosure of classified information
 - Classifies or continues the classification of information contrary to the requirements of E.O. 12958, ISOO Dir No. 1, or this handbook
 - Creates or continues a Special Access Program contrary to the requirements of E.O. 12958
- Security Infraction: Any unintentional action contrary to the requirements of E.O. 12958, ISOO Dir No. 1, or this handbook

1-301 Incident Reporting Procedures

1. Any individual who has knowledge of a security incident shall:
 - Report the circumstances of the incident within 24 hours, in writing, to the immediate supervisor, the assigned NSI Representative, or the NSI Program Team
 - Notify the successive supervisor within the office if the incident involves the direct supervisor or NSI Representative
 - Notify the Director, SMD if the circumstances of discovery warrant such notification impractical to ensure proper security
2. The supervisor or NSI Representative shall:
 - Immediately notify the NSI Program Team
3. The NSI Program Team shall:
 - Assign an individual to conduct a Preliminary Inquiry (PI) to gather the facts surrounding a security incident using the format provided in Appendix B
 - The PI shall be forwarded to the NSI Program Team within 72 hours
 - Review the PI report to ensure it contains factual statements of pertinent information
 - Provide an assessment report to Director, SMD with recommendations for corrective action
 - Retain PI reports for five years from the date of the report, unless law or regulation requires a longer period
4. The Director, Security Management Division shall:
 - Ensure infractions and violations of security requirements, laws, and regulations are promptly investigated
 - Notify or refer security incidents, when required, to appropriate authorities and management officials
 - Make a determination based upon the following:
 - If the inquiry concludes the issue can be resolved without further investigation or the allegation is unfounded, the case may be closed
 - If the inquiry indicates that a formal internal investigation is required, notify Office of Inspector General (OIG) to appoint an investigator who is not involved directly or indirectly in the incident and has an appropriate security clearance

- If a violation of criminal statute is suspected, suspend any further inquiry and refer the case promptly to the appropriate law enforcement agency; notify the Administrator EPA, AA OARM, Director OAS, OIG, and General Counsel
- Forward a letter to the appropriate manager or contracting officer containing a summary of the security incident and required corrective actions to preclude further incidents

Section 4: Administrative Sanctions

1-400 Federal and Non-Federal Employee Administrative Sanction Requirements

1. EPA has legal and regulatory requirements to protect NSI. In accordance with the EPA Information Resources Management (IRM) Policy Manual, Chapter Eight, all EPA employees are subject to appropriate penalties if they knowingly, willfully, or negligently disclose NSI to unauthorized persons. Administrative sanctions shall be coordinated with the Human Resources Office and shall be consistent with the terms of EPA's IRM Policy Manual, EPA Order 3120.1 and any other applicable laws or Agency policies.
2. Non-Federal personnel who knowingly, willfully, or negligently disclose classified information to unauthorized persons may be subject to appropriate laws and sanctions.

Section 5: Reports

1-500 Reporting Requirements

1. The Director, SMD shall establish procedures for the collection and reporting of data necessary to fulfill requirements set forth in the ISOO implementing directives. At a minimum, the Director, SMD shall submit a consolidated report every fiscal year concerning the state of the NSI Program in accordance with ISOO Dir. No. 1.
2. The NSI Representatives are responsible for the submission of an Annual NSI Data Collection Report, provided in Appendix C, to the NSI Program Team. Annual submissions are due by September 30th of each year.

Section 6: Self-Inspection, Program Assessments, and Inspections

1-600 Requirements

The NSI Program Team will establish and maintain an ongoing program to evaluate the implementation and management of EPA's NSI Program. This program will consist of self-inspections, assessment visits, and inspections.

1-601 Self-Inspections

To evaluate the local implementation of this handbook, the NSI Representatives shall conduct an annual self-inspection for their area of responsibility by completing the Self-Inspection Checklist, provided in Appendix D. The completed checklist shall be

forwarded to the NSI Program Team by September 30th of each year. The NSI Representative will maintain a copy of the checklist for two years.

1-602 Assessment Visits

During the development and implementation phase of the NSI Program, the NSI Program Team shall conduct periodic assessment visits of the Programs and Regions. The assessment shall include:

- A review of local procedures, guidelines, and instructions
- A review of infrastructure (i.e., secure rooms and processing equipment) that supports the NSI Program
- A review of access and control records and procedures
- A review of classified holdings
- Interviews with producers, users, and managers of classified information
- Training will be provided based upon deficiencies noted during the visit

1-603 Inspections

Commencing in FY 2008, the NSI Program Team will conduct formal inspections of the Program Offices and Regions to evaluate the implementation against the established standards of this Handbook. The inspection cycle is expected to be conducted every three years.

Section 7: Emergency Release of Classified Information

1-700 Emergency Release of Classified Information

1. The authority to release classified information in an emergency situation rests solely with the Administrator, EPA or the Deputy Administrator. Further delegation of emergency release responsibility can only be authorized, in writing, by the Administrator, EPA.
2. In an emergency situation, and when necessary to respond to an imminent threat to life or in defense of the homeland, the releasing authority shall authorize a disclosing official to release classified information to an individual(s) who is/are otherwise not eligible for access.
3. Emergency release of information pursuant to this authority does not constitute the declassification of the information released.
4. Under these conditions, the disclosing official shall:
 - Limit the amount of classified information disclosed; the information should be provided only to the individuals necessary to achieve the intended purpose
 - Transmit the classified information via approved Federal Government channels by the most secure and expeditious method possible, or by other means deemed necessary when time is of the essence

- Provide instructions about what specific information is classified, the level of classification, and how it should be safeguarded
- Ensure physical custody of classified information remains with an authorized Federal Government representative in all but the most extraordinary and unique circumstances
 - If a custodial change occurs, each change of custody shall be documented and receipted
- Provide appropriate briefings to the recipients on their responsibilities not to disclose the information, and obtain a signed nondisclosure agreement (SF 312)
 - In emergency situations requiring immediate verbal release of information, the signed nondisclosure agreement documenting the briefing may be received after the emergency abates
- Notify the Director, SMD and the originating agency (at the earliest opportunity permitting, but not more than seven days after the release) of the emergency release of classified information. This notification will include:
 - A description of the disclosed classified information
 - Name(s) and contact information of the individuals to which the information was disclosed
 - How the information was disclosed
 - Justification for the emergency release
 - Location of the information and how the information is being safeguarded
 - A description of the de-briefings provided to uncleared individuals
 - A copy of the signed nondisclosure agreements

This page is intentionally blank

Chapter 2: SECURITY CLASSIFICATION

Section 1: Overview

2-100 Overview

This chapter defines principles and concepts required to originally and derivatively classify National Security Information (NSI).

Section 2: Original Classification

2-200 Classification Principles

Because of its nature, certain information must be maintained in a protected manner through a classification system. Information may not be classified unless its disclosure could reasonably be expected to cause damage to national security. The unauthorized disclosure of classified information can cause irreparable damage to national security and loss of human life. E.O. 12958 provides the only basis for classifying NSI.

2-201 Classification Standards

1. Information may only be originally classified under the terms of E.O. 12958 when all of the following conditions are met:
 - An Original Classification Authority (OCA) classifies the information
 - The information is owned by, produced by or for, or is under the control of the U.S. Government
 - The OCA determines that the unauthorized disclosure of the information could reasonably 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
 - The information falls within one or more of the categories of information listed in Section 2-204
2. Classified information shall not be automatically declassified as a result of any unauthorized disclosure of identical or similar information.

2-202 Classification Levels

1. NSI shall be classified by an authorized OCA at one of the following levels:
 - Top Secret shall be applied to information that could reasonably be expected to cause *exceptionally grave damage* to the national security if disclosed to unauthorized sources
 - Secret shall be applied to information that could reasonably be expected to cause *serious damage* to the national security if disclosed to unauthorized sources
 - Confidential shall be applied to information that could reasonably be expected to cause *damage* to the national security if disclosed to unauthorized sources

2. Except as specifically provided by statute, no additional terms such as "Sensitive," "Agency," "Business," or "Administratively" shall be used in conjunction with any of the three classification levels defined above.

2-203 Original Classification Authority

1. Based on E.O. 12958, the authority to classify original information at the Secret or Confidential level may be exercised only by the Administrator, EPA and officials to whom such authority has been directly delegated by the Administrator, in writing, and in accordance with paragraphs 2 through 6 below. Currently, no EPA official is authorized to classify original information at the Top Secret level.
2. The authority to classify original information in EPA may be delegated, in writing, only to those positions with a demonstrable and continuing need to exercise such authority. Incumbents, delegated this authority, occupying these positions must have a security clearance commensurate with the level of original classification authority delegated by the Administrator.
3. The delegation of original classification authority will be limited to the minimum number of officials required for efficient administration and protection of EPA programs. Requests for OCA shall be made to the Administrator through EPA's Office of Homeland Security. The request shall identify:
 - Proposed recipient by position and office
 - Level of classification authority requested
 - Justification for the OCA delegation
4. Requests for OCA shall be granted only when:
 - Original classification is required during the normal course of operations in the Agency
 - Sufficient expertise and information is available to the prospective OCA to permit effective classification decision-making
 - The need for original classification cannot be eliminated by issuance of classification guidance by existing OCAs
 - Referral of decisions to existing OCA at higher levels of management or supervision is not practical
5. OCA delegated by the Administrator cannot be re-delegated.
6. A person assuming a position that has been delegated OCA will assume the delegation, and may make original classification decisions. Prior to making an original classification decision, the person assuming the position must complete OCA training provided by the NSI Program Team. The OCA training requirements are detailed in Chapter 7, Section 401.
7. All original classification and declassification decisions must be reported annually to ISOO through the Director, SMD, using reporting procedures outlined in Chapter 1, Section 1-500.

2-204 Classification Categories

1. Information may be classified when it can be categorized under Section 1.4 of E.O. 12958. The categories are as follows:
 - 1.4(a) Military plans, weapons systems, or operations
 - 1.4(b) Foreign government information
 - 1.4(c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology
 - 1.4(d) Foreign relations or foreign activities of the United States, including confidential sources
 - 1.4(e) Scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism
 - 1.4(f) U.S. Government programs for safeguarding nuclear information or facilities
 - 1.4(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, which includes defense against transnational terrorism
 - 1.4(h) Weapons of mass destruction
2. It is expected that most of the information classified within EPA will be categorized by 1.4(e) or 1.4(g).

2-205 Limitations and Prohibitions

Information shall not be classified to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of national security
- Classify basic scientific research information not clearly related to national security

2-206 Documents Proposed for Original Classification Decisions

1. Information pending an original classification decision will be at the commensurate level of the proposed classification.
2. In cases where an employee or non-federal personnel develops information requiring classification, but does not have the authority to originally classify information, the individual shall mark the information with the proposed classification followed by the words "Pending Original Classification Decision." Marking details are provided in Chapter 4, Section 4-501.
3. The proposed classified information shall be forwarded to the appropriate OCA for an original classification decision. The OCA will have 30 days from receipt of the classification request to make a decision.

4. If it is not clear which OCA within EPA has classification responsibility for the subject information, the information shall be forwarded, with appropriate recommendations, to the Director SMD, for a determination as to which OCA has primary subject matter responsibility.
5. If EPA does not have primary subject matter responsibility, the Director, SMD will forward the information to the Director, ISOO to determine which Federal Agency may make an appropriate original classification decision.
6. Detailed procedures for the classification process are documented in the "Original Classification Process: A Quick Reference Guide" provided by the NSI Program Team.

2-207 Duration of Classification

1. Each time an OCA classifies information, a determination must be made about the duration of the classification.
2. At the time of classification, the OCA shall:
 - Attempt to determine a date or event that is less than 10 years from the date of original classification
 - If unable to determine a date or event of less than 10 years, the OCA shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision
 - 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
3. If an OCA has assigned a date or event for declassification that is less than 25 years from the date of classification, 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 origination, if warranted. To the best extent possible, all recipients will be notified of any classification extensions.
4. In previous executive orders, the OCA was allowed to exempt certain information from declassification. Under E.O. 12958 exemption categories X1 through X8 were withdrawn and can no longer be used. When these markings appear on information dated before September 22, 2003, the information shall be declassified 25 years from the date of the original decision, unless it has been properly exempted under Chapter 3, Section 3-300.

2-208 Security Classification/Declassification Guides

1. A security classification guide shall be developed for each system, plan, program, or project in which classified information is involved. Classification guides also serve as declassification guides. The NSI Program Team will provide a template for classification guides for use within EPA.

2. Security classification guides shall:
 - Identify the subject matter of the classification guide
 - Identify specific items, elements, or categories of information to be protected
 - State the specific classification to be assigned to each item or element of information and, when useful, specify items of information that are unclassified
 - Provide declassification instructions for each item or element of information
 - State a concise reason for classification for each item, element, or category of information that, at a minimum, cite the applicable classification category(ies) in Section 2-204, and the original classification date
 - Identify any special handling requirements that apply to items, elements, or categories of information
 - Identify by name or personal identifier, and position title, the OCA approving the guide and the date of approval
 - Provide a point-of-contact for questions about the guide and suggestions for improvement
 - Provide the date of issuance or last review
3. The Subject Matter Expert (SME) from the program office or facility is responsible for development of the security classification guide. The guide must be submitted in final draft form to the NSI Program Team to ensure compliance with E.O. 12958. The NSI Program Team will forward the final draft to EPA's Office of Homeland Security for review and processing for approval by the OCA.
4. Security classification guides will be approved in writing by the OCA authorized to classify the information. Copies of the guides will be distributed by the originating organization to those organizations and activities believed to be derivatively classifying information covered by the guide or have a valid need-to-know. The original copy of each guide shall be forwarded to the NSI Program Team for permanent retention.
5. Guides shall be revised whenever necessary to promote effective derivative classification. When a guide is revised, computation of declassification dates will continue to be based on the date of the original classification decision. All revisions will be forwarded to the NSI Program Team to determine if action is required by the OCA.
6. At a minimum, guides must be reviewed every five years for continued currency. Upon completion of a review, the guide shall be annotated with the date of the review and forwarded to the NSI Program Team.
7. Classification guides shall be canceled only when all information specified as classified by the guide has been declassified.

2-209 Reclassification of Information

In making the decision to reclassify information that has been declassified and released to the public under proper authority, the Administrator, EPA or the SAO must determine, in

writing, that reclassification of the information is necessary in the interest of national security.

- The Agency must deem the information to be reasonably recoverable, which means that:
 - Most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved
 - If the information has been made available to the public via means such as Government archives or reading rooms, it is withdrawn from public access
- The agency originating the information is authorized to declassify and release information
 - Once the reclassification action has occurred, it must be reported to ISOO within 30 days
 - The notification must include how the “reasonably recoverable” decision was made, including the number of recipients or holders, how the information was retrieved, and how the recipients or holders were briefed
- Any recipients or holders of the reclassified information who have current security clearances shall be appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure
- The recipients or holders who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information that they have had access to, their obligation not to disclose the information, and be requested to sign an acknowledgement of this briefing
- The reclassified information must be appropriately marked and safeguarded and distributed to offices with the need-to-know
- The markings shall include the reclassification authority, the date of the action, and other markings as described in Chapter 4

2-210 Downgrading Classified Information

Information designated a particular level of classification may be assigned a lower classification level by the OCA. Prompt notice of such downgrading must be provided to known holders of the information. The overall classification markings and the classification markings on each page shall be lined through and the appropriate downgraded marking applied. A statement shall be placed on the cover or first page of the document to identify the OCA who made the downgrading determination by name, title, and the date of downgrading decision.

2-211 Classification Challenges

1. To promote proper classification actions, authorized holders of classified information who believe that the classification status of the information is improper are encouraged and expected to challenge the information's classification level. An authorized holder is any individual, including individuals external to the Agency, who have been granted access to specific classified information.
2. Classification challenges shall be considered separately from Freedom of Information Act (FOIA) or other declassification requests.

3. Authorized holders, coordinated with the NSI Program Team, shall present challenges, in writing, to an OCA who has jurisdiction over the information. The challenger shall include a statement indicating why the information should not be classified or should be classified at a different level; however, the challenge need not be any more specific than to question why information is or is not classified or is classified at a certain level.
4. Classification challenge requests shall be submitted to:
 - U.S. Environmental Protection Agency
 - National Security Information Program Team
 - 1200 Pennsylvania Ave, NW
 - Mail Code 3206R, Room G.1-1
 - Washington, DC, 20460
5. EPA is not required to process a challenge on information that has been the subject of a challenge within the past two years, or the subject of pending litigation
6. Classification challenges shall be handled as follows:
 - The NSI Program Team shall maintain a system for processing, tracking, and recording formal classification challenges made by authorized holders
 - Records of challenges shall be subject to oversight by ISOO's, Interagency Security Classification Appeals Panel (ISCAP)
 - The NSI Program Team shall ensure that each challenge is forwarded to EPA's Office of Homeland Security for review and processing by an OCA with jurisdiction over the challenged information
 - The OCA reviewing a classification challenge shall provide a written response to a challenger, via the NSI Program Team, within 60 days
 - If the OCA is unable to complete the classification challenge review within 60 days, the OCA must notify the NSI Program Team and provide a reasonable date to complete the review
 - If the challenger is not satisfied with the decision, the challenger may request a review by an impartial official or panel assigned by the Director, SMD
 - The NSI Program Team will inform the challenger of the OCA's expected timeframe and inform him/her that if no response from the OCA is received within 120 days, he/she has the right to forward the challenge to ISCAP for a decision
 - The challenger may also forward the challenge to ISCAP if the NSI Program Team has not responded to an internal appeal within 90 days of receipt of the appeal
 - Denied challenges shall include, at a minimum:
 - A concise reason for denial of the challenge, unless such reason would reveal additional classified information
 - The names or titles of the officials reviewing the challenge
 - The challenger's rights to appeal
 - The NSI Program Team shall inform the challenger of his or her appeal rights

7. Challengers and the OCA should 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 this handbook. Information being challenged on the basis of classification shall remain classified until a final decision is made to declassify the information.
8. The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be used as a means of minimizing the number of formal challenges.
9. At no time will an individual who challenges a security classification be subject to retribution.

Section 3: Derivative Classification

2-300 Derivative Classification Principles

1. Derivative classification is incorporating, paraphrasing, re-stating, or generating in new form, information that is already classified. Marking the newly developed information must be consistent with the classification markings that apply to the source information.
2. The duplication or reproduction of existing classified information is not derivative classification, and must be treated in the same manner as the originally classified information.
3. With the appropriate security clearance, EPA employees involved in the production or generation of information based on previously classified information are authorized to derivatively classify information without conferring with the OCA.
4. The overall classification markings and portion markings of the source document shall supply adequate classification guidance to the derivative classifier. If portion markings or classification guidance are not found in the source document and no reference is made to an applicable classification guide, guidance should be obtained from the originator of the source document. If such markings or guidance are not available, the derivative classifier shall classify the extracted information using the overall classification of the source document.

2-301 Derivative Classification Procedures

1. Personnel applying derivative classification to classified information shall observe all original classification decisions, carry forward the pertinent classification markings to newly created documents, and apply the date or event for declassification that corresponds to the longest period of classification when the information is based on multiple sources.

2. Derivative classifiers must carefully analyze the information to be classified to determine what information it contains or reveals, and evaluate that information against the instructions provided by the classification guidance or the markings on source documents.
3. Drafters of derivatively classified documents shall portion mark their drafts and keep records of the sources they use to facilitate derivative classification of the finished product.
4. When information is derivatively classified based on "multiple sources" (i.e., more than one security classification guide, classified source document, or combination), the derivative classifier must compile a list of the sources used. A copy of this list must be included in or attached to the file or record copy of the document.
5. If the derivative classifier has reason to believe the classification applied to information is inappropriate, the classifier of the source document shall be contacted to resolve the issue. The information will continue to be classified as specified in the source document until the matter is resolved.
6. If the office originating the classified information no longer exists, the office that inherited the functions of the originating office is responsible for determining the action to be taken with respect to declassification. If the functions of the originating office were dispersed amongst multiple offices and the inheriting office(s) cannot be determined, or the functions have ceased to exist, the senior official of which the originating activity was a part is responsible for determining the action to be taken with respect to classification.

This page is intentionally blank

Chapter 3: DECLASSIFICATION

Section 1: Overview

3-100 Overview

This chapter defines the principles and concepts required to declassify information and explain how to use the scheduled, automatic, systematic, and mandatory declassification processes.

Section 2: General

3-200 Requirement

1. The authority to declassify or downgrade information classified by EPA may be exercised only by the Administrator, EPA and officials to whom such authority has been delegated (i.e., OCAs) in accordance with Chapter 2.
2. Information shall be declassified when it no longer meets the standards for classification. In some exceptional cases, the need to protect information through continued classification may be outweighed by the public interest to disclose the information. In these cases, the information should be declassified. When such questions arise, they shall be referred to the Administrator, EPA or the Senior Agency Official (SAO) who will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.
3. E.O. 12958 established four systems of declassification:
 - Scheduled Declassification A system requiring the original classifier to decide, at the time information is classified, when it can be declassified. Guidance can be obtained in Chapter 2, Section 2-206
 - Automatic Declassification A system that will cause classified information of *permanent historical value* to be automatically declassified on the 25th anniversary of its classification unless specific action is taken to keep it classified. Guidance is provided in Section 3-300
 - Systematic Declassification Review A system to review records containing classified information that have a *permanent historical value* and have been exempted from automatic declassification. Guidance is provided in Section 3-301
 - Mandatory Declassification Review A system for reviewing classified information for possible declassification in response to a request that meets the requirements under the FOIA, Privacy Act of 1974, and the provisions of this handbook. Guidance is provided in Section 3-302

Section 3: Declassification Systems

3-300 Automatic Declassification

1. On December 31, 2006, all classified information and records that are more than 25 years old and are determined to have *permanent historical value* under Title 44 of the United States Code, shall be automatically declassified unless exemption has been granted from Interagency Security Classification Appeals Panel (ISCAP).
2. All classified information or records classified prior to issuance of E.O. 12958 shall be automatically declassified on December 31 of the year, 25 years from the date of its original classification, except as provided in the exemption review process provided in paragraph 4.
3. Classified information and records that have not been scheduled for disposal or retention by the National Archives and Records Administration (NARA) are not subject to the automatic declassification provisions of E.O. 12958.
4. The Administrator, EPA or the SAO may propose to exempt specific information from records that have permanent historical value from automatic declassification if the release could be expected to:
 - Reveal the identity of a confidential human source or a human intelligence source, or reveal information about the application of an intelligence source or method
 - Reveal information that would assist in the development or use of weapons of mass destruction
 - Reveal information that would impair U.S. cryptologic systems or activities
 - Reveal information that would impair the application of state-of-the-art technology within U.S. weapon systems
 - Reveal current U.S. military war plans that remain in effect
 - Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government or seriously and demonstrably undermine ongoing diplomatic activities of the United States
 - Reveal information that would clearly and demonstrably impair the current ability of U.S. Government officials to protect the President, Vice President and other officials for whom protection services, in the interest of national security, are authorized
 - Reveal information that would impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures or projects relating to the national security
 - Violate any statute, treaty or international agreement
5. The exemption proposal shall be submitted to ISCAP within five years of but no later than 180 days before the information is subject to automatic declassification. The proposal shall include:
 - A description of the information or file series, either by reference to information in specific records or in the form of a declassification guide

- An explanation of why the information is exempt from automatic declassification and must remain classified for a longer period
 - A specific date or event for declassification of the information
6. The ISCAP may direct EPA not to exempt the information or to declassify it at an earlier date than recommended. Appeals of such a decision shall be submitted to the Director, ISOO. The information will remain classified while such an appeal is pending.
 7. Information or records exempted from automatic declassification shall remain subject to systematic and mandatory declassification review provisions.

3-301 Systematic Declassification Review

1. Records containing information that have *permanent historical value* and have been exempted from automatic declassification shall be subject to systematic declassification.
2. The Director, SMD is responsible for identifying classified EPA information containing *permanent historical value*, 25 years and older, and still require protection. These records are maintained at NARA.

3-302 Mandatory Declassification Review

1. To meet the requirements under the FOIA, Privacy Act of 1974, and the provisions of this handbook, any individual or organization may request a review of classified information for declassification under E.O. 12958. The NSI Program Team shall ensure that requests for declassification are processed in accordance with the provisions of those laws.
2. All information classified under E.O. 12958 or predecessor orders shall be subject to a review for declassification by EPA if the following criteria are met:
 - The request for a review describes the document or material, containing the information, with sufficient specificity to enable EPA to locate it with a reasonable amount of effort
 - The information is not exempted from search and review under sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403-5c, 403-5e, and 431)
 - The information has not been reviewed for declassification within the past two years
 - If EPA has reviewed the information within the past two years, or the information is the subject of pending litigation, EPA shall inform the requester of this fact and of the requester's appeal rights
3. Mandatory declassification review requests shall be processed as follows:
 - Classified information under EPA jurisdiction must be reviewed for declassification upon receipt of a request

- Requests shall be submitted to:
 - U.S. Environmental Protection Agency
 - National Security Information Program Team
 - 1200 Pennsylvania Ave, NW
 - Mail Code 3206R, Room G.1-1
 - Washington, DC, 20460
- A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient specificity to allow the office with primary responsibility to locate the records containing the information sought with a reasonable amount of effort
- The NSI Program Team shall acknowledge receipt of the request directly to the requester. The NSI Program Team shall ensure that each mandatory declassification review is forwarded to EPA's Office of Homeland Security for review and processing by an OCA with jurisdiction over the information
 - The OCA conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification described in Chapter 2
 - When information cannot be declassified in its entirety, the person declassifying the information will make a reasonable effort to declassify as much as possible (this is known as redaction)
- The OCA must review the information within 30 days
 - The OCA shall inform the NSI Program Team of the declassification determination or request additional time
- The OCA shall make a final declassification determination within 180 days from the date of receipt
- The NSI Program Team shall communicate its declassification determination to the requester
 - If the request is denied, the requester will be informed of the right of an administrative appeal which must be filed within 60 days of receipt of the denial
 - a. Requesters have the right to appeal the OCA's decision of EPA to ISCAP in accordance with E.O. 12958
- Following the receipt of an appeal, the NSI Program Team shall make a determination within 90 days
 - If additional time is required, the requester will be informed of the additional time needed and provide the requester with the reason for the extension
- The NSI Program Team shall notify the requester, in writing, of the final determination and the reasons for any denial

4. When EPA receives a mandatory declassification review request for records in its possession that were originated by another agency, the NSI Program Team shall refer the request and the pertinent records to the originating agency or department. However, if the originating agency has previously agreed that the custodial office may review its records, the custodial office 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 NSI Program Team shall process the request in accordance with this chapter.

This page is intentionally blank

Chapter 4: IDENTIFICATION AND MARKING

Section 1: Overview

4-100 Overview

This chapter defines the principles and concepts and explains the requirements for marking and identifying classified information.

Section 2: General

4-200 Requirements

Marking is the principal means of informing holders of classified information and of the specific protection requirements for the information. All classified information must be clearly identified by classification markings.

4-201 Marking Standards

1. Overall Markings Conspicuous labels are required at the top and bottom of the front cover page, title page, outside back cover, and first page with the highest overall classification level of the information contained in the document. The front cover, title page and first page must also include the date the document was finalized, and portion markings on the subject or title.
2. Classification Block Every classified document (original or derivative) shall contain a classification block on the front cover, title page, or first page in the lower left corner.
3. Interior Page Markings Conspicuous labels are required at the top and bottom of each page with the highest overall classification level of the information contained on the page, or with the highest overall classification of the document, including the designation "UNCLASSIFIED" when it is applicable.
4. Portions Marking Each subject line, title, paragraph, subparagraph, section (i.e., classified diagram, map, drawing, etc.) or similar portion of a classified document shall be marked to show the classification level of that portion or to indicate that it is unclassified. Specifically, the following information must be included:
 - Each section, part, paragraph, and similar portion of a classified document shall be marked to show the highest classification level of information it contains, or that it is unclassified
 - Portions of text shall be marked with the appropriate abbreviation ("TS," "S," "C," or "U"), placed in parentheses immediately before the beginning of the portion
 - If the portion is numbered or lettered, place the abbreviation in parentheses between the letter or number and the start of the text
 - The portion marking that precedes the subject or title indicates the classification of the subject or title, not the classification of the document

- When possible, select unclassified subjects and titles of classified documents
 - Place the portion markings for subjects and titles of classified documents immediately preceding the subject or title
 - Mark illustrative information (i.e., graph, table, chart, or figure) of a classified document with the highest classification level of the contents contained in the illustrative information
 - Portion mark the title of the illustrative information
5. A Classification Marking Quick Reference Guide has been produced by the NSI Program Team to provide basic illustration of marking requirements. The guide is available for download at <http://intranet.epa.gov/oas/smd/ns-guides.htm>.

Section 3: Original Classification Markings

4-300 Required Original Classification Markings

1. Information originally classified shall bear all markings prescribed in Section 4-201.
2. At the time of original classification, the following information shall appear on the face of each classified document (this information is also referred to as the classification block):
 - **Classified By:**
 - The OCA shall cite a personal identifier such as name, position, and office symbol
 - **Reason:**
 - The OCA shall state the reason for the decision to classify the information
 - At a minimum, the classifier shall include a brief reference to the pertinent classification category as listed in E.O. 12958, Section 1.4 and identified in Chapter 2, paragraph 2-204
 - **Declassify On:**
 - The "Declassify On" line shall include the duration of the original classification decision
 - The classifier shall apply one of the above instructions according to the declassification decision made based on the guidance set forth in Chapter 2, Section 2-206

4-301 Marking Examples for Originally Classified Information

1. John Smith, the EPA Laboratory Director, has been delegated OCA for scientific research in his laboratory by the Administrator, EPA. On October 10, 2002, he has determined that a scientific experiment relating to an EPA operation in his lab needs to be classified until completion of the operation. The operation will be complete in less than 2 years. He will mark this decision on all applicable classified research documents as follows:

Classified By: John Smith, Director, EPA Laboratory

Reason: 1.4 (e)

Declassify On: Completion of Operation

2. On October 10, 2002, the OCA has determined that a scientific experiment relating to an EPA operation in the lab needs to be classified for seven years. The OCA will mark this decision on all applicable classified research documents as follows:

Classified By: (OCA name and position)

Reason: 1.4 (e)

Declassify On: October 10, 2009

3. When a specific date or event is not identified, the OCA shall apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 10, 2002, mark the "Declassify On" line as follows:

Classified By: (OCA name and position)

Reason: 1.4(e)

Declassify On: October 10, 2012

4. If the OCA determines that the information requires protection beyond the original date, the "Declassify On" line shall be revised to include the new declassification instructions, the identity of the OCA authorizing the extension, and the date of the action. This date cannot exceed 25 years from the date of the original document or classification decision. An example of an extended duration of classification is as follows:

Classified By: (OCA name and position)

Reason: 1.4 (e)

Declassify On: October 10, 2009 (Classification extended on October 10, 2009 until December 1, 2015, by (OCA name and position))

Section 4: Derivative Classification Markings

4-400 Required Derivative Classification Markings

1. Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in Section 4-201. Source document markings shall be carried forward or taken from appropriate classification guides.
2. At the time of derivative classification, the following information shall appear on the face of each classified document (this information is also referred to as the classification block):

Derived From: State Department Memorandum dated October 5, 1993
Subject: IT Developments

Declassified On: Source marked OADR, date of source October 5, 1993

4. On October 12, 2003, a cleared employee is drafting a memorandum derived from an Air Force source document (Subj: New Laser Gun) dated December 2, 2000. The source document has "X4" on the "Declassify On" line.

Derived From: Air Force Memorandum dated December 2, 2000
Subject: New Laser Gun

Declassified On: Source marked X4, date of source December 2, 2000

5. Multiple source documents are utilized to create an EPA memorandum. A different declassification date is specified on each document. The date that corresponds with the longest period of time among the sources is December 31, 2019 (When using multiple sources, list those sources on a separate document and attach to the official file copy).

Derived From: Multiple Sources

Declassify On: December 31, 2019

Section 5: Additional Marking Requirements

4-500 Marking Prohibitions

1. Markings other than such as "For Official Use Only," "Sensitive But Unclassified," "Limited Official Use," "Law Enforcement Sensitive," or "Sensitive Security Information" shall not be used to identify NSI.
2. Terms such as "Secret Sensitive," "Confidential Business Information," or "Agency Confidential," shall not be used to identify NSI.
3. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify non-classified information.

4-501 Documents Proposed for Original Classification

Information pending an original classification decision will be safeguarded in a manner commensurate to its proposed classification.

1. Conspicuously label the top and bottom of the front page or cover page with the proposed highest level of classification followed by the words "Pending Original Classification Decision."
2. Portion mark all pages and include the date the document was created on the first page.

4-502 Transmittal Documents

Mark an unclassified transmittal document with the highest classification level of any attached information. If the transmittal document is unclassified, mark it with the appropriate instruction (i.e., “THIS DOCUMENT IS UNCLASSIFIED WHEN SEPERATED FROM ITS CLASSIFIED ATTACHMENT(S)”). If the transmittal letter contains classified information, mark it appropriately and ensure the classification instruction states the classification level of the transmittal letter once separated from its classified attachment.

4-503 Files, Folders, and Binders

1. Classified cover sheets, SF 703 (Top Secret), SF 704 (Secret), or SF 705 (Confidential), shall be affixed to the exterior cover of files, folders, and binders that contain classified information. Each standard form shall be used according to the highest classification of the contents.
2. Classified cover sheets shall be affixed each time a classified document is handled or when stored in an appropriate container.
3. The only occasion when a cover sheet does not need to be affixed to an individual document is when the document is placed in a folder or binder with other classified documents where the appropriate cover sheet is affixed to the exterior identifying the highest level of the documentation contained within the folder or binder.
4. If a cover sheet is not available, mark or stamp the files or folders with the highest classified information contained within.

4-504 Classified Working Papers

Working papers are defined as draft documents or information, which are expected to be edited or revised prior to becoming a finalized product and released outside the originating agency. Working papers include classified notes.

1. They may be retained for 180 days, after which they must be marked in the same manner prescribed for a finished document at the same classification level.
2. The top and bottom of each page shall be labeled with the words WORKING PAPER and the highest classification level of the information contained on the page.
3. On the first page, include the date that the document was created, originator’s name and program office, and portion mark applicable paragraphs.

4-505 Charts, Maps, Graphs, and Drawings

Charts, maps, graphs, and drawings must bear the appropriate overall classification marking under the legend, title block, or scale. Portion marking shall be used to indicate the highest level of classification of the legend or title itself. The highest level of classification shall be labeled at the top and bottom of each document. The originator must apply additional markings that are clearly visible when the document is folded or rolled.

4-506 Photographs, Films, and Recordings

Photographs, films (including negatives), recordings, and their containers shall be marked to alert a recipient or viewer that the information contains classified information.

1. Photographs Negatives and positives shall be marked whenever practicable with the appropriate classification level, authority, and declassification instructions. The classification level shall be marked at the beginning and end of each strip. All markings shall be placed on containers of negatives and positives. When self-processing film or paper is used to photograph or reproduce classified information, the classifier must remove all parts of the last exposure from the camera and destroy them as classified waste, or the camera should be protected as classified information. If possible, mark the face side of a print with the appropriate classification level and declassification instructions. Markings that cannot be applied to the face side shall be stamped on the reverse side or affixed by pressure tape label, stapled strip, or other comparable means.
2. Transparencies and Slides Classification markings shall be shown clearly on the image of each transparency or slide or on its border, holder, or frame.
3. Motion Picture Films Classified motion picture films and video tapes shall be marked at the beginning and end of each reel with titles bearing the appropriate classification. Reels must be kept in containers bearing clear classification, declassification, and downgrading markings (if applicable).
4. Recordings Sound, magnetic, or electronic recordings shall contain a clear statement of the assigned classification level at the beginning and the end. Recordings must be kept in containers or on reels that bear clear classification, declassification, and downgrading markings (if applicable).
5. Microfilm or Microfiche Microfilm or microfiche contain images in sizes too small to be read by the naked eye. The classification must be marked clearly on the microfilm medium and its container, so it is readable by the naked eye. In addition, these markings must be included on the image so that when the image is displayed or printed, the markings shall be clean and readable.

4-507 Information Used for Training Purposes

Unclassified information used to simulate classified documents or information for training purposes shall be marked: "[Classification] for training purposes only, otherwise Unclassified."

4-508 Automated Information Technology (IT) Storage Media

1. Storage media (i.e., hard drives, diskettes, floppies, etc.) that contain classified information shall bear external classification markings and internal notations indicating the classification level.

2. Exterior labels shall be used to mark magnetic or digital media, other non-paper media, and equipment for which cover sheets are not feasible.
3. The following standard forms shall be affixed to each item, depending on the classification: SF 706 (Top Secret), SF 707 (Secret), SF 708 (Confidential), and SF 710 (Unclassified). SF 710s labels are required for use in open storage areas, but are not required when stored outside the open storage area. Sample labels are provided in Appendix E.
4. All media in storage containers used for classified information must have the appropriate classification level affixed.
5. Additional marking requirements for classified information systems are provided in Chapter 10.

4-509 Classified Documents Produced by Classified Information Systems

Each page produced by information systems equipment that is authorized to process classified information shall bear appropriate classification markings. Complete documents created on these systems shall be marked in accordance with Chapter 4, Section 2.

Section 6: Declassification Markings

4-600 General

A uniform security classification system requires that standard markings be applied to declassified information. Markings shall be clearly applied leaving no doubt about the information's declassified status and who authorized the declassification.

4-601 Procedures

The following markings shall be applied to documents, records, or copies of records, regardless of media:

- The word, "Declassified"
- The name or personal identifier, and position title of the declassification authority or declassification guide
- The date of declassification
- The overall classification markings that appear on the cover page or first page shall be lined through with a straight line
- Example:

~~**SECRET**~~ **DECLASSIFIED**

Declassified By: (OCA name and position or declassification guide/document)

Declassify On: October 10, 2004

Chapter 5: SAFEGUARDING

Section 1: Overview

5-100 Overview

This chapter defines the principles and concepts required to safeguard classified collateral information including access, document control, storage, reproduction, and destruction requirements. It also defines the requirements and procedures for accreditation of secure areas.

Section 2: General

5-200 Requirements

1. Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.
2. Authorized persons who have access to classified information are responsible for:
 - Protecting it from unauthorized access
 - Securing it in approved containers or spaces whenever it is not under the direct control of an authorized person
 - Meeting the safeguarding requirements of this handbook
 - Ensuring that classified information is not communicated over unsecured voice or data circuits, in public, or in any other manner that permits interception by unauthorized persons

Section 3: Access

5-300 General Restrictions on Access

1. A person may have access to classified information provided that:
 - A favorable determination of eligibility for access to classified information has been made
 - The person has signed an SF 312, Non-Disclosure Agreement
 - The person has a valid need-to-know
2. No employee has a right to gain access to classified information solely by virtue of title, position, or level of security clearance.
3. The final responsibility for determining whether an individual obtains access to classified information rests with the individual who has possession, knowledge, or control of the information and not with the prospective recipient. Before classified information is disclosed, the holder must:
 - Verify the recipient's identification
 - Verify the recipient's security clearance
 - Determine the recipient's valid need-to-know
 - Advise the recipient of the classification level of the information

Section 4: Document Accountability and Review

5-400 Policy

Top Secret information will be controlled via written records or electronic database and accounted for annually by the NSI Representative. Secret and Confidential information will be reviewed annually by the NSI Representative.

5-401 Top Secret Document Accountability

1. All Top Secret (including copies) originated or received by an office shall be continuously accounted for, individually serialized, and entered into the NSI Representative's Top Secret log.
2. The log shall include the date originated or received, individual serial number, copy number, title (unclassified if possible), originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified), and date of each disposition.
3. Top Secret information shall be inventoried annually, at the change of the NSI Representative, and/or upon the report of loss or compromise. During the annual inventory, each document must be visually inspected to determine possible downgrade, declassification, or required destruction. One complete copy of the Top Secret inventory will be forwarded to the NSI Program Team by September 30th of each year.
4. The Classified Information Accountability Record, provided in Appendix H, shall be used to record transmission, reproduction, and destruction of Top Secret, and shall be maintained for five years.

5-402 Secret and Confidential Document Review

1. Stringent control measures shall be in place for Secret and Confidential information.
2. Each document must be visually inspected to determine possible downgrade, declassification, or destruction of classified holdings to reduce the amount necessary for operational and program purposes.
3. Control measures include external receipts and dispatch records to ensure that documents are tracked during transmission.
4. The Classified Information Accountability Record, provided in Appendix H, shall be used as a record of receipt, and shall be maintained for two years.

5-403 Return of Classified Information

1. All cleared personnel leaving their positions or the Agency, shall account for all classified information in their possession and transfer it to a person who has a valid need-to-know and the appropriate security clearance.
2. The NSI Representative, through a formalized local process, shall verify that all classified information has been properly transferred.

Section 5: Storage**5-500 Policy**

1. Classified information must be stored under conditions that will provide adequate protection and prevent access by unauthorized persons. Whenever classified information is not under the personal control and observation of an authorized person, it must be stored in an accredited open storage area or in a GSA approved class 5 or 6 (legal or letter size) security container located in secure areas as defined in Chapter 5, Section 6.
2. A security container or vault shall not bear any external markings, which may reveal the level of classified information authorized, stored, or priority for emergency evacuation or destruction. This does not preclude placing a mark or symbol on the container for other purposes (e.g., identification and/or inventory number or barcode).
3. An office that receives classified information and has no authorized storage equipment available must do one of the following:
 - Return the classified information to the sender
 - Arrange with another office to properly store the information
 - Destroy it by an approved method
4. Classified information shall not be left unattended, in an unauthorized storage container, taken to a personal residence, or placed in the custody of a person who does not have the proper security clearance or a valid need-to-know.
5. Weapons or sensitive items such as cash, jewels, precious metals, or drugs, shall not be stored in the same container used to safeguard classified information.

5-501 Storage Standards

1. GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.
2. The Director, SMD may determine more stringent requirements are needed based on the volume, nature, and sensitivity of the information to be protected in relation to other factors, such as types of containers, presence of guards, vault-type space, or intrusion alarms.

5-502 Storage of Classified Information

1. Top Secret information shall be stored by one of the following methods:
 - In a GSA-approved class 5 or 6 (letter or legal) security container with one of the following supplemental controls:
 - 24 hour protection by a cleared guard
 - Inspection of the locked security container shall be checked every two hours by cleared guard or duty personnel
 - An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm activation
 - Security-In-Depth conditions provided the container is equipped with a lock meeting Federal Specification FF-L-2740
 - In an accredited open storage area
2. Secret or Confidential information shall be stored by one of the following methods:
 - In the same manner as prescribed for Top Secret information
 - In a GSA-approved class 5 or 6 (letter or legal) security container without supplemental controls located in secure areas as defined in Chapter 5, Section 6

5-503 Combinations

1. Access to Combinations
 - Only appropriately cleared and authorized employees shall have access to combinations
 - The number of employees who have access to the combination shall be kept to the absolute minimum
 - The owner of the security container and an alternate (if possible) shall be clearly identified on each SF 700, Security Container Information Form
 - These employees are to be notified in the event the container is found unsecured
2. Protecting Classified Combinations
 - The classification of combinations shall be at the highest level of classified information that is protected by the lock
 - Any written record of the combination shall be marked with the appropriate classification level and protected at that level
 - Combinations are not to be recorded on calendars, on rolodex lists, in desk drawers, in key-locked filing cabinets, in wallets, or stored at home
3. Maintaining Container Information and Classified Combinations
 - SF 700s will be maintained for each locking drawer of a container
 - The SF 700 must be stored in a separate container
 - If the NSI Representative does not have the means to store the combination in this manner, send the SF 700 to the NSI Program Team
 - The SF 700 for Top Secret combinations shall be accounted for, individually serialized, and entered into the Top Secret accountability log.

4. Changing Classified Combinations
 - Combinations to locks shall be changed only by personnel with the appropriate security clearance and a valid need-to-know for access to the classified information
 - Combinations shall be changed:
 - Whenever placed into service
 - Each time a person with knowledge of the combination no longer requires access to it
 - When the combination has been subject to possible compromise
 - When a container is taken out of service, it shall be inspected by the NSI Representative to ensure that no classified information remains
 - The lock shall be reset to the standard combination of 50-25-50 prior to removal from the office space

5-504 End of Day Checks

An SF 701, Activity Security Checklist, provided in Appendix E, shall be placed in the proximity of the main door to serve as a daily reminder to secure classified information and equipment at the end of the day. The SF 701 shall be modified to include a listing of all security related items that need to be checked in the space prior to close of business (e.g., secure phone key, safes, burn bags, computer media, printer, desks).

5-505 Security Container Check Sheet and Open/Closed Signs

1. An SF 702, Security Container Checklist, provided in Appendix E, shall be placed on the exterior of each classified security container and open storage area to record each time the container/area is locked or unlocked.
2. The individual who conducts the end-of-day check must ensure the container is properly locked and secured by pulling on the handles of the drawers and then spinning the combination dial at least four rotations. Although it is not always possible, the person conducting the end-of-the-day check should not be the same person who locked or unlocked the security container during the duty day.
3. Reversible magnetic OPEN-CLOSED signs, or similar signs, shall be used as reminders on all classified storage containers each time they are locked or unlocked.

Section 6: Types of Secure Areas

5-600 Principles and Concepts

1. This section defines the principles and concepts governing the construction and protection of secure areas for the purpose of storing, processing, handling, and discussing classified NSI. Secure areas are defined as follows:
 - Open Storage Accredited Areas
 - Areas used for continuous handling, storing, reviewing, discussing, and processing classified information

- Secure Accredited Area
 - Areas used for non-continuous handling, reviewing, storing (within a GSA approved container), discussing and processing classified information up to and including Top Secret (e.g. offices, meeting rooms, laboratories)
 - Restricted Areas
 - Temporary areas established to control access from unauthorized disclosure while handling or reviewing classified information in non-accredited areas
2. Accreditations are required prior to the use of both open storage and secure areas.
 3. Accreditations will be conducted in accordance with Section 5-601 and approved by the NSI Program Team. The Team will maintain a database of all accredited areas and their accreditation status.
 4. Accreditations are valid of one year; thereafter, requiring recertification to remain in use for classified operations.
 5. The accreditation officials may impose more stringent standards if conditions and circumstances are warranted following a risk assessment.
 6. Accreditation is not required for restricted areas; however, designation and approval shall be granted by the NSI Representative prior to use.

5-601 Accreditation Procedures

The following procedures shall be applied to obtain an accreditation of an Open Storage or Secure Area:

1. Accreditation The requester shall complete the Room Accreditation Checklist, provided in Appendix F, and submit it to the NSI Representative. The NSI Representative shall ensure the checklist is complete, verify the information is correct, then forward it to the NSI Program Team for review and approval. Upon approval, the NSI Program Team will issue an accreditation, in writing, to the NSI Representative. The NSI Representative shall ensure that the room's occupant receives a copy.
2. Recertification Open storage and secure areas require recertification on an annual basis. The NSI Representative will request recertification of all accredited areas in his/her area of responsibility by completing the appropriate information in Section A of the Accreditation Status Form, provided in Appendix G, and forward it to the NSI Program Team. The NSI Program Team will complete the appropriate information in Section B and return it to the NSI Representative authorizing recertification. The NSI Representative shall ensure that the room's occupant receives a copy. The recertification consists of checks for continued compliance of all pertinent policies and procedures.

3. Suspension If the NSI Representative determines classified information might be compromised or that the security conditions are unsatisfactory, he/she will immediately suspend the accreditation, complete the appropriate information in Section A of the Accreditation Status Form, provided in Appendix G, and forward it to the NSI Program Team. (A suspended accreditation means that no classified work can take place until necessary corrections have been made and the area is recertified). The NSI Program Team will complete Section B defining the action required to recertify the area, and return it to the NSI Representative. The NSI Representative shall ensure that the room's occupant receives a copy. When necessary corrections have been made and verified by the NSI Representative, a new Accreditation Status Form shall be completed requesting recertification of the area. The NSI Program Team will recertify the area by completing the appropriate information in Section B and return it to the NSI Representative authorizing recertification. The NSI Representative shall ensure that the room's occupant receives a copy.
4. Withdrawal If an accredited area is no longer required, the NSI Representative will request an accreditation withdrawal by completing the appropriate information in Section A of the Accreditation Status Form, provided in Appendix G, and forward it to the NSI Program Team. The NSI Program Team will complete the appropriate information in Section C and return it to the NSI Representative authorizing withdrawal. The NSI Representative shall ensure that the room's occupant receives a copy.

5-602 Open Storage Accredited Area

Open Storage Accredited Areas are used for continuous handling, storing, reviewing, discussing and processing classified information up to and including Top Secret. Minimum security requirements are listed below.

1. Access:
 - Access shall be controlled to preclude unauthorized entry through the use of a cleared employee or by an access control device or system
 - Access shall be limited to authorized persons who have an appropriate security clearance and a valid need-to-know for the classified information within the area
 - Persons without the appropriate clearance level shall be escorted at all times by an authorized person after the area has been sanitized of all classified information
 - An authorized personnel access roster shall be posted on the backside of the entrance door by the NSI Representative and updated as necessary
 - A visitors log shall be maintained to account for escorted visitors in the space
2. Construction:
 - Construction must be completed to provide visual evidence of unauthorized penetration
 - Perimeter walls will be true floor to true ceiling, permanently constructed, and attached to each other
 - Vents, ducts, and similar openings that are over 6" in its smallest dimension or over 96 sq inches that enter or pass through an open storage area shall be

protected with either 1/2" steel bars six inches on center, expanded metal grills, commercial metal sound baffles, or an IDS

- Doors shall have a solid core and be constructed of wood, metal, or other suitable material
 - Entrance doors shall be secured with a built-in GSA approved three position electronic combination lock (e.g., X-09)
 - A door-sweep, an automatic door closer, and weather stripping around the door is required to prevent discussions being overheard in unapproved areas
 - Emergency exit doors within the room shall be secured from the inside with emergency egress hardware that is building safety code compliant
- Windows shall be made opaque or equipped with blinds, drapes, or other coverings
 - Windows at ground level will be constructed from or covered with material to provide protection from forced entry (e.g., steel bars/mesh)
 - The protection provided to the windows need be no stronger than the strength of the contiguous walls
 - Windows that open and close shall be made inoperable either by sealing them or equipping them on the inside with a locking mechanism
 - The windows will be monitored by an IDS (either independently or by the motion detection sensors within the area)

3. Sound Attenuation:

- The area perimeter walls, doors, windows, floors and ceilings, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of information

4. Secure Phone:

- Secure phones are obtained from the Office of Solid Waste and Emergency Response (OSWER) and are authorized for use at the classification level of the accreditation

5. Classified Processing:

- Classified computer processing is authorized provided the computer has been approved under the National Security Systems Program policy defined in Chapter 10 of this handbook

6. Supplemental Protection:

- An accredited open storage area must have one of the following supplemental controls:
 - 24 hour protection by a cleared guard
 - Inspection of an unoccupied area will be conducted by cleared guards every two hours if accredited for Top Secret information, and four hours if accredited for Secret and Confidential information
 - An IDS with the personnel responding within 15 minutes of the alarm activation for Top Secret information and within 30 minutes for Secret and Confidential information

- Security-In-Depth conditions, as determined by the NSI Program Team Leader, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740

5-603 Secure Accredited Area

Secure Accredited Areas are used for non-continuous handling, storing, reviewing, discussing, and processing of classified information up to and including Top Secret. Open storage is not authorized. When classified information is not in use, it will be secured in an approved class 5 or 6 (letter or legal size) security container. Minimum security requirements are listed below.

1. Access:
 - During the entire period the Secure Accredited Area is in use, the entrance will be controlled and access limited to persons having proper clearance and a valid need-to-know.
2. Construction:
 - Perimeter walls will be permanently constructed and attached to each other
 - True floor to true ceiling is not required
 - Cubical partitions are not considered walls
 - Doors will be constructed of wood, metal, or other suitable material and shall be secured with a cipher or keyed lock
 - All windows which might reasonably afford visual surveillance of personnel, documents, information, or activities within the facility, shall be made opaque or equipped with blinds, drapes or other coverings to preclude visual surveillance
3. Sound Attenuation:
 - The area perimeter walls, doors, windows, floors, and ceilings, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of information
4. Secure Phone:
 - Secure phones are obtained from OSWER and are authorized for use at the classification level of the accreditation
 - If a secure phone is installed, the doors to the space must be locked when unoccupied
5. Classified Processing:
 - Classified computer processing is authorized provided the computer has been approved under the National Security Systems Program policy defined in Chapter 10 of this handbook
6. Secure Storage and Supplemental Protection:
 - Top Secret information shall be stored in a GSA approved security container with one of the following supplemental controls:
 - 24 hour protection by a cleared guard

- Inspection of the security container shall occur every two hours by cleared guard or duty personnel
- An IDS with the personnel responding within 15 minutes of the alarm annunciation
- Security-In-Depth conditions provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740
- Secret information shall be stored by one of the following methods:
 - In the same manner as prescribed for Top Secret information
 - In a GSA approved class 5 or 6 (letter or legal size) security container or vault without supplemental controls

5-604 Restricted Area

Restricted Areas may be established on a temporary basis to control access from unauthorized disclosure while handling or reviewing classified information in non-accredited areas. Classified discussions, storage, and secure phones are not authorized in a Restricted Area. Accreditation is not required for a restricted area; however, designation and approval shall be granted by the NSI Representative, prior to its use. A Restricted Area shall have a clearly defined perimeter, but physical barriers are not required. Cleared personnel within the area shall be responsible for restricting all persons who lack the appropriate clearance and a valid need-to-know. When classified information is not in use, it shall not be left unattended and shall be secured in an approved GSA class 5 or 6 (letter or legal size) security container.

Section 7: Reproduction of Classified Information

5-700 General

This section outlines the security precautions necessary to protect classified and other sensitive information from possible compromise as a result of copy machine use or other duplicating means. New technology available for copy machines increases security vulnerabilities. The term copy machine refers to photocopying machines, facsimile machines, printers that produce hard copy output, electronic blackboards that provide a reproduction of what is written on the board, and any machine with a combination of these functions.

5-701 Requirements

1. Copy machines within the EPA shall be designated as "approved" or "non-approved" for the reproduction of classified information, if they are located at a site that contains both classified and unclassified information. The NSI Representative is designated to authorize copiers within his/her area of responsibility.
2. Designated classified copy machines shall be located in Open Storage Areas only.
3. Digital copiers with electronic chip memory capabilities shall be utilized only in a stand-alone capacity. Digital copiers used to reproduce classified information shall not be connected to any network or telephone line.

4. Remote diagnostic capabilities (i.e., dial-in) of classified copy machines shall not be connected to the telephone wall jack because most copy machines have internal memory which could be accessed remotely.
5. Those machines that contain memory capabilities shall have the memory removed by an authorized cleared person prior to servicing by non-cleared personnel.
6. After designation of a copier as "approved" or "non-approved," it will be clearly identified by a posted notice. Additionally, NSI Representatives will issue a classified copy machine approval letter to the copier's owner. The letter will identify the machine(s) that are approved, the location, and the point-of-contact in the office. The point-of-contact will be required to coordinate with the NSI Representative when potential security problems arise, or when there are incidents of possible compromise.
7. Reproduction of classified information shall be limited to those instances when it is absolutely necessary and authorized by the originator. For accountability purposes, reproduction of Top Secret information requires coordination with the NSI Representative. When Top Secret information is reproduced, the additional copies must be accounted for in the NSI Representative's Top Secret log. Records must be maintained to show the number and distribution of all reproduced Top Secret documents. Secret and Confidential information may be reproduced without prior approval of the originator unless otherwise indicated on the document.

5-702 Procedures

The following procedures shall be adhered to when reproducing classified information:

1. Cleared individuals will remain at the copier until classified reproduction is complete.
2. Before leaving the copier, individuals must check the copier for any copies or originals that may be left in the machine.
3. If the machine malfunctions and the original and/or copy cannot be cleared or retrieved, the NSI Representative shall be notified to ensure that the machine is removed from approved service until the owner certifies that the malfunction has been properly corrected, at which time, the machine may be re-authorized for classified use.
4. The NSI Representative shall be notified of the scheduled service visit and arrange for an appropriately cleared employee to be present. Any documents, image retaining drum sheets, or memory chips must be removed from the machine and shall be collected by the copier's owner. No unescorted maintenance person shall be allowed access to any reproduction equipment used for the reproduction of classified information.

Section 8: Destruction

5-800 Policy

1. Classified documents shall be destroyed in a manner sufficient to preclude recognition or reconstruction of the classified information. The NSI Representative shall establish procedures for the proper destruction of classified information in his/her organization. Such procedures must ensure that authorized destruction methods are used, and that it is properly witnessed and documented on a Classified Information Accountability Record, provided in Appendix H, for Top Secret information. The NSI Representative shall retain Top Secret destruction receipts for 2 years.
2. Classified waste (in any form) shall be appropriately protected at all times. Classified waste is defined as notes (working papers), carbon paper, typewriter and printer ribbons, disks and other material containing classified information.
3. Guidance for the destruction of classified waste resulting from processing on information systems, such as personal computers and printers, can be obtained from the NSI Program Team.

5-801 Authorized Destruction Methods

Classified documents shall be destroyed by shredding.

1. Only National Security Agency (NSA)-approved crosscut shredders, currently listed on the National Security Agency (NSA/CCS) Evaluated Products List (EPL-02-01) of High Security Cross Cut Shredders, shall be used for destruction of classified information.
2. Information shredded to these specifications is considered unclassified.
3. Shredders used for destroying classified information shall be properly marked with appropriate signage to identify its classified usage.

5-802 Unauthorized Destruction Methods

Burning or other methods for destruction, such as melting, chemical decomposition, or mutilation are not authorized within the EPA.

Chapter 6: TRANSMISSION METHODS

Section 1: Overview

6-100 Overview

This chapter defines the principles and concepts required to transmit classified information inside and outside the EPA. Transmission methods include mail, courier, and electronic NSA approved secure telecommunications.

Section 2: General

6-200 Requirements

1. Classified information shall only be transmitted electronically over approved secure telephones, secure facsimile machines, or approved classified information systems.
2. Classified information shall be transmitted and received in an authorized manner which ensures evidence of tampering can be detected; inadvertent access can be precluded, and assures timely delivery to the intended recipient. Individuals transmitting classified information are responsible for ensuring intended recipients are properly cleared and have the capability to store classified information in accordance with the requirements of E.O. 12958.
3. The NSI Representative will ensure that only appropriately cleared personnel or authorized carriers transmit, transport, escort, or hand-carry classified information. Unless a specific form of transmission or transportation is restricted or available, the means selected should minimize the risk of a loss or compromise.
4. The NSI Representative will develop local procedures to ensure the movement of classified information can be tracked, properly disseminated, easily accessible, and quickly detected if lost. The NSI Representative will also develop and implement local procedures to protect incoming mail, bulk shipments, and items delivered by messenger that contain classified information.
5. Acknowledgement of receipt is required for classified information transmitted, transported, or hand-carried in and out of EPA controlled areas. This receipt shall contain only unclassified information that clearly identifies the classified information. Receipts for Top Secret information must be retained for five years; receipts for Secret and Confidential information must be retained for two years. An example of the Classified Information Accountability Record (EPA 1350-2), provided in Appendix H.

Section 3: Packaging for Transmission

6-300 Packaging Requirements for Mailing and Couriering outside EPA

1. All classified information transmitted to other agencies, activities, or facilities shall be enclosed in an opaque inner and outer cover (e.g., sealed envelopes, wrappings, locked briefcase, pouch, or container) which conceals the contents and provides reasonable evidence of tampering. The Classified Information Accountability Record shall be completed for all transmissions of classified information outside the Agency.
2. Material used for packaging must provide durability to protect the contents in transit and prevent items from breaking out of the cover. All seams must be taped to provide visual evidence of tampering.
3. The inner sealed cover shall be clearly marked on both sides with the highest classification of the information contained within, any required protective markings, and complete forwarding and return addresses.
4. The outer sealed cover shall be addressed in the same manner, but shall not bear any classification markings or indication that classified information is enclosed.

Section 4: Methods of Transmission

6-400 Top Secret Information

1. Before transmitting Top Secret information, the sender must coordinate with his/her NSI Representative for control and accountability of the information. Top Secret information shall be transmitted only by using one of the following methods:
 - Direct contact between authorized persons
 - Defense Courier Service (DCS) or a GSA authorized government agency courier service (e.g., FEDEX, UPS)
 - Diplomatic pouch through the Department of State Diplomatic Courier System
 - Designated courier or escort with Top Secret clearance
 - Electronic means via approved Top Secret communications systems
2. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or other commercial courier services.

6-401 Secret Information

Secret information shall be transmitted by one of the following methods:

- Any of the methods established for Top Secret; however, Secret information may be transmitted via the Defense Courier Service (DCS) only when the information cannot be transmitted in U.S. custody by any other means
- A GSA authorized government agency courier service (e.g., FEDEX, UPS)
- U.S. Postal Service Express Mail or U.S. Postal Service Registered Mail

6-402 Confidential Information

Confidential information shall be transmitted by using one of the following methods:

- Any of the methods established for Secret information
- U.S. Postal Service Certified Mail
- When the recipient is a U.S. Government facility, Confidential information may be transmitted via U.S. 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 rather returned to the sender
- Confidential information shall not be transmitted to government contractor facilities via First Class Mail

6-403 Transmissions to a U.S. Government Facility Located Outside the U.S.

1. 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 completed via methods specified in Section 6-400
2. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information, provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system

Section 5: Hand-Carrying Classified Information**6-500 General Policy**

1. Classified information may be hand-carried by cleared EPA employees or non-federal personnel within EPA controlled spaces without a courier card providing information is adequately protected against visual observation (i.e., inside a folder, envelope, or briefcase).
2. The NSI Program Team Leader is the Agency approving official for employees and non-Federal personnel to be couriers of classified information. The courier must be appointed by his/her supervisor, hold an appropriate security clearance, be trained on courier procedures, sign a courier agreement, and possess a valid courier authorization card.
3. As a last resort, classified information may be hand-carried out of the local area or aboard commercial passenger aircraft when there is neither time nor means available to properly transmit the information by other authorized methods. Local area is defined as 75 miles from your designated work location. The Out Of Area Courier Checklist, provided in Appendix I, is required to be completed prior to travel, by both the courier and the NSI Representative, to carry classified information out of the local area or aboard commercial aircraft.
4. The NSI Program Team Leader may grant permission to carry classified information to overseas locations on a case-by-case basis.

6-501 Courier Cards

1. The EPA courier card authorizes the bearer to transport or hand-carry classified information on a recurring basis. The card will identify the holder by name, employee ID number, date and place of birth, issue and expiration date, assigned office code, level of classified information authorized to be hand-carried, the geographical limits authorized to the courier, and the signatures of both the holder and the approving official.
2. The NSI Program Team shall maintain serialized accountability of all courier cards.
3. Appropriately cleared personnel may obtain a courier card subject to the following process:
 - The employee's supervisor shall provide, in writing, justification for issuance of a courier card to the NSI Program Team Leader
 - Upon approval, the NSI Program Team Leader notifies the NSI Representative, in writing, to administer the approved courier briefing and have the designated individual sign the Courier Agreement, provided in Appendix I
 - Upon signature, the Courier Agreement shall be submitted to the NSI Program Team for process and issuance of the courier card
 - The NSI Program Team will forward the courier card to the NSI Representative for the individual's signature and issuance
4. The bearer of the courier card must report the loss or damage of the card immediately to the NSI Representative who, in turn, will notify the NSI Program Team. The bearer may request a replacement card, which will be issued at the NSI Program Team Leader discretion.
5. The courier card is valid for three years from the date of issue for federal employees and one year for non-federal employees.
6. The bearer must return the courier card to the NSI Representative upon termination of security clearance or employment within the agency, contract expiration, authorization is no longer needed, or occurrence dictates the need to withdraw the courier authorization.
7. The courier card does not authorize the courier to hand-carry classified information out of the local area or aboard commercial aircraft. Permission to hand-carry classified information out of the local area or aboard commercial aircraft shall be granted by the NSI Representative in accordance with Section 6-503.

6-502 Courier Requirements and Responsibilities

Appropriately cleared personnel may be authorized to hand-carry classified information outside EPA-controlled spaces subject to the following conditions:

- The courier has an appropriate security clearance and has been issued a Courier Card, in accordance with Section 6-501

- Couriers shall ensure that the information remains in his/her physical possession at all times
- Upon arrival, the courier will transfer the classified information to the authorized government or contracting facility representative who is accepting responsibility for safeguarding the package
- When classified information is hand-carried outside of EPA controlled space, the courier must ensure classified information is double wrapped and appropriately marked
 - An envelope may serve as the inner wrapper, and a locked zipper pouch or locked briefcase may serve as the outer cover
- Classified information shall not be opened, read, studied, displayed, discussed, or used in any manner by the courier when traveling in public conveyances, or at his/her home
- The courier shall not store classified information in any detachable storage compartment, such as automobile trailers, luggage racks, and aircraft overhead bins when carrying classified information in a private, public, or government conveyance
- Prior to hand-carrying classified information, the courier will provide to the NSI Representative a list of all classified information to be hand-carried
- If an overnight stop is required, the courier will make advance arrangements with the NSI Representative for proper overnight storage in an authorized government or contractor facility
- The courier will obtain a signed receipt from an authorized government or contracting facility representative who is accepting responsibility for safeguarding the package
- In the event of any emergency, delay, change in destination, loss or compromise of classified information, the courier will immediately notify his/her NSI Representative or the NSI Program Team
- Emergency contact information is provided on the back of the courier card

6-503 Hand-Carry Authorization for Out of Area or Aircraft Travel

1. Appropriately cleared personnel may be authorized to hand-carry classified information out of local area or aboard commercial passenger aircraft subject to the following conditions:
 - When there is neither time nor means available to properly transmit the information by other authorized methods
 - When written authorization is provided to the courier from the NSI Representative
2. If travel out of the local area is required, the NSI Representative shall:
 - Complete an Out of Area Courier Preparation Checklist, provided in Appendix I, with the courier
 - Issue an Authorization to Transport Classified Government Information aboard a Commercial Aircraft memorandum, sample provided in Appendix I, (if applicable)

6-504 Authorization to Hand-Carry Information to an Overseas Location

Appropriately cleared personnel may be authorized to hand-carry classified information overseas subject to the following conditions:

- Written authorization from the NSI Program Team Leader via the NSI Representative
- The courier must ensure the information will not be opened or viewed by customs, border, postal, or other inspectors, either U.S. or foreign
- The courier must travel aboard a U.S. carrier
 - Foreign carriers can only be used when no U.S. carrier is available
- The courier must ensure that the information remains in his/her custody and control at all times
- The NSI Representative shall brief the courier concerning security safeguards while couriating overseas and the need to possess EPA photographic identification

Chapter 7: SECURITY EDUCATION AND TRAINING

Section 1: Overview

7-100 Overview

This chapter establishes security education and training requirements for all personnel whose duties involve access to classified National Security Information.

Section 2: General

7-200 Roles and Responsibilities

1. Standardized training materials are developed and maintained by the NSI Program Team and are offered on a scheduled and as required basis.
2. The NSI Representatives shall provide required security education and training to employees assigned within their Program Offices and Regional locations.
3. The Director, SMD may expand or modify the coverage provided in this chapter according to Agency, program, or policy needs.

Section 3: Initial Orientation Training

7-300 Initial Orientation

1. All employees in the Agency who are cleared for access to classified information must attend an initial orientation to the NSI Program before accessing classified information.
2. The NSI Representative shall administer initial orientation training.
3. The initial orientation shall, at a minimum, address the following:
 - Roles and responsibilities
 - Senior Agency Official
 - Security Management Division
 - NSI Representatives
 - Cleared EPA personnel
 - Elements of classifying and declassifying information
 - Classified information and why it requires protection
 - Levels of classified information and the damage criteria associated with each level
 - Prescribed classification markings and their importance
 - General requirements for declassifying information
 - Procedures for challenging the classification status of information
 - Elements of safeguarding
 - Proper procedures for safeguarding classified information
 - Unauthorized disclosure and the criminal, civil, and administrative sanctions associated with disclosures

- General conditions and restrictions for access to classified information
 - Responsibilities when safeguarding standards may have been violated
 - Methods for dealing with uncleared personnel who work in proximity to classified information
4. At the completion of the initial orientation training, the NSI Representative shall:
- Obtain the employee's signature indicating agreement to the terms of the Classified Information Nondisclosure Agreement (SF 312)
 - Sign the Witness and Acceptance section of the SF 312
 - Mail the originally signed SF 312 to the NSI Program Team
 - The NSI Program Team will forward the SF 312 to OARM's Personnel Security Branch to retain in the employee's security personnel file

Section 4: Specialized Security Training

7-400 General

Agency personnel in specified roles in the NSI Program shall be provided specialized security education and training sufficient to permit performance of those duties. The education and training shall be provided before, concurrent with, or not later than six months following placement in those positions.

7-401 Original Classification Authorities

The security training provided shall, at a minimum, address the following:

- Differences between original and derivative classification
- Delegation of OCA authority
- Standards that an OCA must meet to classify information
- Discretion that an OCA has in classifying information
- Process for determining duration of classification
- Prohibitions and limitations on classifying information
- Basic markings that must appear on classified information
- General standards and procedures for declassification
- Standards for creating and using Agency classification/declassification guides

7-402 NSI Representatives

The security training provided shall, at a minimum, address the following:

- Original and derivative classification standards and processes
- Proper and complete classification markings to be applied to classified information
- Methods and processes for downgrading and declassifying information
- Methods for the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information
- Requirements for creating and updating classification and declassification guides
- Requirements for controlling access to classified information
- Procedures for investigating and reporting instances of actual or potential compromise of classified information

7-403 Courier Training

1. The NSI Representative shall administer courier training to employees or non-federal personnel appointed courier responsibilities.
2. All appointed personnel shall receive training that, at a minimum, addresses the following:
 - Safeguarding practices and procedures
 - Courier requirements
 - Emergency situations
3. Administrative procedures for the issuance of a courier card are detailed in Chapter 6, Section 6-501.

7-404 Other Types of Training

Additional security education and training shall be required for personnel who:

- Use the original and derivative classification procedures
- Grant or represent classified contracts
- Use classified information systems
- Participate in international programs that are governed by security requirements
- Are approved for access to Special Programs

Section 5: Annual Refresher Security Training**7-500 Annual Refresher Training**

1. The NSI Representative shall administer the annual refresher training to all cleared employees and non-federal personnel.
2. All cleared employees and non-federal personnel must participate, annually at a minimum, in refresher training that reinforces policies and procedures of the NSI Program.
3. At the completion of the training, the NSI Representative shall:
 - Email or fax the NSI Program Team indicating the employee's full name and date trained

Section 6: Termination Briefings**7-600 Termination Briefings**

1. The NSI Representative shall conduct a termination briefing to all cleared employees who leave the Agency or whose security clearance is terminated or withdrawn.

2. At a minimum, termination briefings shall address the following:
 - The obligation to return to the appropriate Agency official all classified information in the employee's possession
 - The continuing responsibility not to disclose any classified information to which the employee had access
 - The potential penalties for non-compliance
3. At the completion of the debriefing, the NSI Representative shall:
 - Obtain the employee's signature in the security debriefing acknowledgement section of a Classified Information Nondisclosure Agreement (SF 312)
 - Mail the originally signed SF 312 to the NSI Program Team
 - The NSI Program Team will forward the SF 312 to OARM's Personnel Security Branch to retain in the employee's security personnel file

Chapter 8: FOREIGN GOVERNMENT INFORMATION

Section 1: Overview

8-100 Overview

This chapter defines the principles, standards, and concepts required for safeguarding information classified by foreign governments.

Section 2: Protection of Foreign Government Information

8-200 General

1. Foreign Government Information (FGI) is provided to the United States by a foreign government, international organization of governments, or produced by the United States through a written combined arrangement, that requires either the information or the arrangement be kept in confidence.
2. The unauthorized disclosure of FGI is presumed to cause damage to national security; therefore, it shall retain its original classification designation and be assigned a U.S. classification level that will ensure a degree of protection equivalent to that provided by the originator of the information. Appendix J contains a detailed list of security classification markings to be used when deriving the equivalent U.S. classification level.
3. This chapter is not applicable to North Atlantic Treaty Organization (NATO) designated classified information. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions.

8-201 Requirements for Safeguarding Foreign Government Information

1. The requirements described in this chapter are additional baseline safeguarding standards that may be necessary for FGI that requires protection pursuant to an existing treaty, agreement, bilateral exchange, or other obligation.
2. To the extent practical, and to facilitate 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.
3. The safeguarding standards described below may be modified, if required, by treaties or agreements, or for other obligations with the prior written consent of the national security authority of the originating government, hereafter referred to as the “originating government.”

8-202 Safeguarding Foreign Government Information

1. Receipt, internal distribution, destruction, access, reproduction, and transmittal records for Top Secret FGI will be maintained. Reproduction requires the consent of the originating government and destruction of the information must be witnessed.

2. Receipt, internal distribution, destruction, access, reproduction, and transmittal records for Secret FGI will be maintained. It may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless the originating government waives this requirement.
3. Receipts for records marked Confidential need not be maintained for Confidential FGI unless required by the originating government.
4. To ensure the protection of other FGI provided in confidence (e.g., foreign government “Restricted,” “Designated,” or unclassified provided in confidence), the information must be classified and safeguarded under E.O. 12958. The receiving agency or non-federal personnel (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:
 - Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet purposes served by U.S. classification markings
 - Mark documents “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level)” if foreign markings are not adequate
 - The notation, “Modified Handling Authorized,” may be added to either the foreign or U.S. markings authorized for FGI
 - If remarking foreign originated documents is impractical, approved cover sheets may be an authorized option
5. Documents shall be provided only to those who have a valid need-to-know, and where access is required by official duties.
6. Individuals allowed access shall be informed of applicable handling instructions through a briefing, written instructions, or applying specific handling requirements to an approved cover sheet by the applicable program office.
7. Documents shall be stored in a manner to prevent unauthorized access commensurate to the appropriate classification level.

8-203 Transmission Methods

1. Transmission shall take place between designated government representatives using the transmission methods described in Chapter 6.
2. When classified information is transferred, via the Classified Information Accountability Record, provided in Appendix H, to a foreign government or its representative, a signed receipt is required and shall be maintained for two years.
3. Documents shall be transmitted via an approved classified information transmission method, unless waived by the originating government.

8-204 Marking Foreign Government Information

In addition to the marking requirements detailed in Chapter 4, the following additional requirements apply to FGI:

- Derivatively created documents that contain FGI shall be marked: **"This Document Contains [*indicate country of origin*] Information."** The portions of the document that contain the FGI shall be marked to indicate the government and classification level (e.g., "UK-C").
- If the specific foreign government must be concealed, the documents shall be marked: **"This Document Contains Foreign Government Information"** and pertinent portions shall be marked "FGI" together with the classification level (e.g., "FGI-C"). In such cases, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions. If FGI must be concealed, the markings should not be used. The document should be marked as if it were of U.S. origin.
- When classified records are transferred to the National Archives and Records Administration (NARA) for storage and archival purposes, the accompanying documentation shall identify the portions that contain FGI.
- Documents need not be re-marked as FGI when they bear foreign government markings.

8-205 Declassification of Foreign Government Information

1. The declassifying agency is the agency that initially received or classified the information. The declassifying agency or the Department of State, as appropriate, will consult with the foreign government(s) prior to declassification.
2. When FGI appears to be subject to automatic declassification, the declassifying agency shall determine if the information is subject to a treaty or international agreement preventing declassification at that time.

8-206 Third Party Release

The release or disclosure of FGI to any third country entity must have the prior consent of the originating government. Consent can be obtained with an exchange of letters or written into a treaty, agreement, bilateral exchange, or other obligation.

This page is intentionally blank

Chapter 9: INDUSTRIAL SECURITY

Section 1: General

9-100 Overview

This chapter establishes the roles, responsibilities, requirements, and procedures for EPA's participation in the National Industrial Security Program (NISP). This chapter supplements the provisions of the NISP Operating Manual (NISPOM).

9-101 Authority

The contents of this handbook are derived from the following:

- Executive Order (E.O.) 12829, "National Industrial Security Program", dated January 6, 1993; herein after referred to as E.O. 12829
- DoD 5522.22-M, National Industrial Security Program Operating Manual, dated February 2006
- Federal Acquisition Regulation (FAR), dated March 2005

9-102 Policy

1. Executive Order 12829, entitled "National Industrial Security Program" (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States 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.
2. DoD 5522.22-M, entitled "The National Industrial Security Program Operating Manual" (NISPOM) incorporates the requirements of E.O. 12829. It provides baseline standards for the protection of classified information, released or disclosed to industry, in connection with classified contracts under the NISP. It is applicable to all EPA contractors, licensees, certificate holders, or grantees that access NSI through contractual obligations.
3. The Federal Acquisition Regulation (FAR), Subchapter A, Part 4, Subpart 4.4 provides Federal Government implementation provisions when a contract requires access to classified information. The provisions require a Contract Security Classification Specification (DD 254) be prepared and distributed during all phases of contracting activity.

Section 2: Program Management

9-200 Roles and Responsibilities

1. The Assistant Administrator, Office of Administration and Resources Management, as the Senior Agency Official (SAO), shall:
 - Direct and administer EPA's Industrial Security Program
 - Account each year for the costs within the agency associated with the implementation of the National Industrial Security Program
2. The Director, Security Management Division, shall:
 - Be responsible for policy development, implementation, interpretation, administration, and program oversight
 - Furnish assistance and guidance to contracting and program personnel relating to the security requirements of any action involving classified information
 - Assist the Contracting Officer and/or Contracting Officer Representative with the development of the Contract Security Classification Specification (DD 254)
3. The Contracting Officer (CO), shall:
 - Ensure all solicitations and contracts comply with the policies and procedures identified in this chapter and the requirements of the Federal Acquisition Regulation (FAR) and the NISPOM regarding the safeguarding of classified information
 - Coordinate with the Contracting Officer Representative and the NSI Representative to ensure classified information in the possession of contractors, and pertaining to contracts, is afforded applicable safeguards
 - Ensure that contractual security specifications, safeguards, and/or protection requirements are coordinated with the NSI Program Team
 - Approve the DD 254s, to include the following actions:
 - Ensure all DD 254s have been presented to the NSI Program Team Leader for certification prior to approval
 - Issue a revised DD 254 whenever a modification or additional classification guidance is necessary
 - Review the existing classification specification during the term of the contract or, at a minimum, once every two years
 - Issue a final DD 254 upon completion of the contract
4. The Contracting Officer Representative (COR), shall:
 - Prepare DD 254s for the CO's approval
 - Verify the contractor's facility clearance (FCL) status
 - Contact the NSI Program Team, through the NSI Representative, to verify an FCL
 - If a contractor does not have an FCL, provide sponsorship to DSS to initiate the FCL granting process
 - Verify the contract employees' personnel clearance (PCL) status and valid need-to-know prior to granting access to classified information or EPA spaces where classified information will be disclosed

5. The NSI Representative, shall:
 - Maintain records of contractor/consultant personnel in his/her Program or Region subject to the NISP (i.e., DD 254 and visit certifications)
 - Identify classified information unique to classified contract for incorporation into the DD 254
 - Provide assistance and guidance to the CO and the COR, with respect to industrial security matters, in his/her Program or Region
 - Ensure that all personnel assigned to a classified contract at EPA have been briefed on the contents of this handbook and any applicable Standard Operating Procedures (SOPs) for their work location

Section 3: Requirements

9-300 General

1. The President designated the Secretary of Defense as Executive Agent for the NISP. The Defense Security Service (DSS) administers the NISP on behalf of the Executive Agent. Policy, procedures, standards, and training for the NISP are available at the DSS web site <http://www.dss.mil>.
2. The Director, Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP, and for reviewing implementation regulations, internal rules, or guidelines on all signatories. EPA is a signatory to and participates in the National Industrial Security Program.
3. Participation in the NISP allows EPA to use DSS to conduct investigations for contractor facility and personnel security clearances and to monitor the contractor's compliance with safeguarding requirements. All facility and personnel security clearances granted by DSS will be accepted by EPA to establish eligibility for access to classified information.
4. The requirements prescribed for a classified contract are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other government Agency program or project which require access to classified information by the contractor.

9-301 Security Requirement Contract Clause

The CO shall include a security requirements clause in solicitations and contracts when the contract may require access to classified information. Specific clauses are listed in the FAR, at 52.204-2.

9-302 Contract Security Classification Specification (DD 254)

1. The FAR, subpart 4.4, requires a Contract Security Classification Specification (DD 254) to be incorporated in each classified contract. The DD 254 is the primary means for relating contract specific security classification guidance to the contractor

and shall prescribe the source(s) from which classification requirements can be derived.

2. In most instances, the DD 254 will be unclassified. In those instances where it is necessary to include classified information in the DD 254, it must be marked accordingly and protected in a manner commensurate with its classification level.
3. Specific instructions on completing the DD 254 are available from the NSI Program Team.
4. Once the DD 254 has been prepared by the COR and reviewed by SMD, it will be sent to the CO for signature and inclusion in the contract or solicitation.
5. The NSI Program Team will maintain a copy of all EPA DD 254s.

9-303 Contractor Eligibility Requirements

1. Facility Security Clearance (FCL) Prior to the disclosure of any classified information to a contractor, the responsible COR must obtain verification that the contractor's facility is in possession of a valid FCL equal to or higher than the level of classified information to be disclosed in the performance of the contract.
 - A FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted
 - The FCL may be granted at the Confidential, Secret, or Top Secret level
 - The FCL includes the contractor execution of a DoD Security Agreement (DD 441) to abide by the security requirements set forth in the NISPOM
 - Requests for certification shall be submitted, in writing, to the NSI Program Team and shall contain the following information:
 - Name and location of the contractor facility
 - Brief description of the work to be performed
 - Level of access to classified information required
 - A statement whether the facility is to receive, generate, use, and/or store classified information in the performance of the contract
 - The estimated volume of classified information segregated by classification level, to be provided to, and/or generated by, the contractor
 - The name and telephone number of the point of contact at the contractor facility who is knowledgeable and responsible for the contract
2. Government Sponsorship A contractor or prospective contractor cannot apply for its own FCL. A government contracting activity, or a currently cleared contractor, may sponsor an uncleared company for an FCL. Sponsorship request letters shall be on agency letterhead and shall include the requestor's name and address, a justification, and the classification level of the FCL. The letter shall be mailed to: DISCO, Attn: Facilities Division, 2780 Airport Drive, Suite 400, Columbus, OH 43219-2268. A company must meet the following eligibility requirements before it can be processed for an FCL:

- The company must need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement
 - The company must be organized and existing under the laws of any of the fifty states, the District of Columbia, or Puerto Rico, and be located in the United States or its territorial areas
 - The company must have a reputation for integrity and lawful conduct in its business dealings
 - The company and its key managers must not be barred from participating in U.S. Government contracts
 - The company must not be under foreign ownership, control, or influence (FOCI) to such a degree that the granting of the FCL would be inconsistent with the national interest
3. Personnel Security Clearance (PCL) A PCL is an administrative determination that an industrial employee is eligible for access to classified information. This determination is based on an investigation and review of available personal data, and a finding that access is clearly consistent with national interests. Contractors must have clearances commensurate with the level of access required for performance under the contract.
- The Defense Industrial Security Clearance Office (DISCO), a field element of DSS, issues personnel security clearances under the authority of the NISP, for contractors
 - The contractor's Facility Security Officer (FSO) must provide the COR a visit certification, which includes the reason for the visit and verification of employee's clearance
 - The COR or the NSI Representative will verify the clearance and need-to-know before granting the contractor access to any classified information
 - The contractor's FSO is responsible for passing security clearances of contracted employees for visits to other classified facilities

Section 4: Visits and Meetings

9-400 Visits and Meetings

1. Classified Visits The government employee hosting a meeting with contractors shall ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information. The host shall ensure that visitors are only afforded access to classified information consistent with the purpose of the visit.
2. Clearance Verification The Joint Personnel Adjudication System (JPAS) is available for verifying incoming contractor's PCL; however, if the use of such a database is not available, a Visitor Authorization Letter (VAL) may still be used. Specific requirements for a VAL can be found in paragraph 6-104 of the NISPOM.

This page is intentionally blank

Chapter 10: NATIONAL SECURITY SYSTEMS PROGRAM

Section 1: General

10-100 Overview

This chapter sets forth the roles and responsibilities, standards, guidelines, and procedures for classified information systems designated National Security Systems at the Environmental Protection Agency (EPA). It is applicable to all EPA employees and non-federal personnel that have a requirement to process collateral (Top Secret, Secret, and Confidential) classified information.

10-101 Authority

- E-Gov Act of 2002, Title III, Federal Information Security Management Act (FISMA)
- Computer Security Act of 1987
- Office of Management and Budget - Circular No. A-130, Appendix III
- National Security Directive No. 42 (NSD-42)
- Committee on National Security Systems (CNSS) policies, directives, instructions, and advisory memorandums
- EPA Delegation 1-6-A, National Security Information
- EPA Information Resources Management (IRM) Policy Manual, Chapter 8

10-102 Policy

1. All personnel with classified information systems security responsibilities must adhere to the current laws, directives, and regulations for national security systems in addition to standards, guidelines, and procedures of this chapter when EPA information systems are used to support collateral (Top Secret, Secret, and Confidential) classified processing requirements.
2. This chapter is not applicable to Sensitive Compartmented Information (SCI) and Special Access Program (SAP) processing requirements. Authority for SCI and SAP are provided in:
 - SCI - Director of Central Intelligence Directive 6/3 (DCID 6/3)
 - SAP - Joint Air Force, Army, Navy Manual 6/3 (JAFAN 6/3)

10-103 Security Incident Reporting

If classified information is found, loaded, or inadvertently processed on an unclassified computer or any computer attached to the EPA's unclassified intranet, the incident will be reported immediately in accordance with EPA's Computer Security Incident Response Capability (CSIRC) procedures. Immediate reporting is essential to minimize the impact to classified/unclassified systems or networks. Reporting is conducted as follows:

1. Immediately, report the incident, verbally, to the Information Systems Security Representative (ISSR). If there is suspicion of criminal activity, personnel will also contact EPA IG/CCD at 202-566-2588.

2. The ISSR will verbally report to the Information Systems Security Officer (ISSO) and the EPA CSIRC via the EPA Call Center phone number at 1-866-411-4EPA (4372).
3. The ISSR will forward a written report to the ISSO and the EPA CSIRC to provide documentation of the incident.

Section 2: Program Management

10-200 Roles and Responsibilities

EPA's Information Resources Manual, Chapter 8, through the authority of EPA Delegation 1-6-A, defines the responsibility of establishing and implementing standards and procedures for classified NSI in accordance with EPA information security policy and all applicable Federal laws, regulations, and executive orders. Individual roles and responsibilities are depicted in Figure 1 and defined in the paragraphs below.

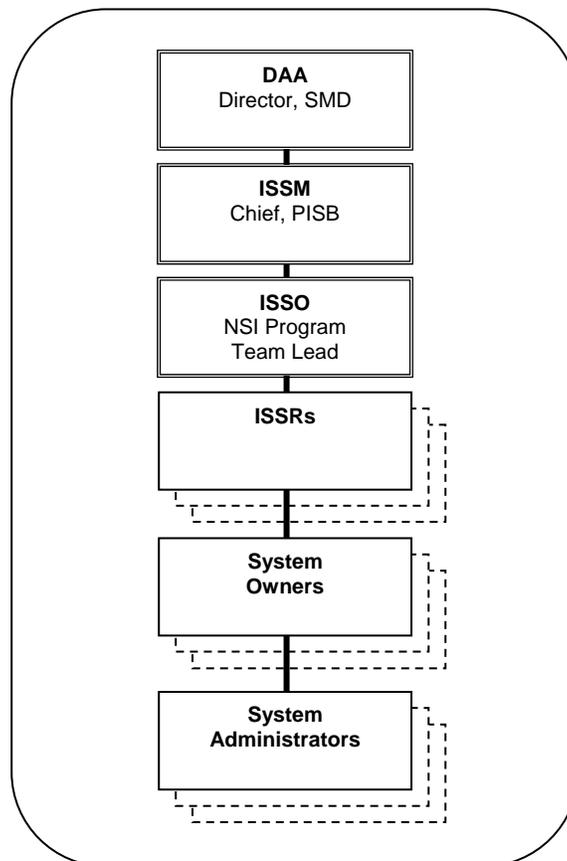


Figure 1. Roles and Responsibilities Hierarchy

1. Designated Approval Authority (DAA)
The Director, SMD is designated the DAA for EPA. The DAA grants formal approval to operate EPA sponsored classified information systems based on the systems operating environment, sensitivity levels, and mitigating safeguards documented in the System Security Authorization Agreement (SSAA). The approval shall be a written, dated statement that clearly sets forth any conditions or restrictions

to system operation. The DAA has the authority to withdraw approval, suspend operations, grant interim approval to operate, or grant variations to security when circumstances warrant.

2. Information Systems Security Manager (ISSM)

The Physical and Infrastructure Security Branch Chief is designated as the ISSM for EPA. The ISSM is responsible to provide oversight of EPA's National Security Systems Program (NSSP). The ISSM shall:

- Approve NSSP standards, guidelines, and procedures
- Ensure periodic reviews are conducted to ensure the program is implemented and effective
- Ensure independent evaluation of National Security Systems is conducted and reported annually to Director of the Office of Management and Budget (OMB) in accordance with FISMA, and in cooperation with current EPA reporting procedures
- Ensure a current inventory and tracking system is in place and reported annually in accordance with Federal Regulations

3. Information System Security Officer (ISSO)

A staff member of the NSI Program Team is designated the ISSO. The ISSO shall possess a clearance equal to or higher than the highest classification of data stored or processed on all EPA classified information systems. This position must be approved in writing by the ISSM. The ISSO is responsible for ensuring that security is maintained for classified information systems. The ISSO shall:

- Draft NSSP standards, guidelines, and procedures
- Provide guidance for developing Systems Security Authorization Agreements (SSAA), System Security Plans (SSP), and Memorandums of Agreement (MOA) for use with classified information systems
- Provide guidance for approval of classified information systems
- Review SSAAs, SSPs, and MOAs
- Draft security awareness and training for EPA's National Security Systems Program (NSSP)
- Conduct periodic compliance reviews of Programs and Regions
- Coordinate with the ISSRs and System Administrators to ensure proper implementation of approved security features

4. Information System Security Representative (ISSR)

The ISSR assists the ISSO in the Programs and Regions and is responsible for making a technical judgment that classified information systems are in compliance with the stated requirements of the approved security plan. ISSR activities shall be performed by competent technical personnel and will function independently (i.e., separation of duties) from the System Administrator. The ISSR shall possess a clearance equal to or higher than the highest classification of data stored or processed on systems in his/her designated Program and Region. This position must be approved in writing by the ISSM. The ISSR shall:

- Conduct certification of eligible systems based on the requirements listed in the approved SSAA
- Ensure System Owners and System Administrators maintain systems in compliance with the approved SSAA
- Conduct audits on installed security features
- Conduct security awareness and training

5. System Owner

The System Owner is responsible for the procurement and daily operation of his/her classified information system. The System Owner shall possess a clearance equal to or higher than the highest classification of data stored or processed on classified systems owned. The System Owner, although not typically responsible for performing daily security activities, is responsible for ensuring that they are implemented and maintained. The System Owner shall:

- Designate a System Administrator that has a security clearance equal to the highest level of classified information that will be stored or processed on the system
 - EPA HQ shall utilize the System Administrator assigned to the NSI Program Team
- Advise the ISSO of any special protection requirements for information to be processed on the system
- Determine the processing application(s) essential for the system to fulfill the program mission
- Write the required SSAAs, SSPs, and MOAs related to his/her own system
- Ensure configuration management procedures for hardware and software upgrades are maintained by the System Administrator
- Ensure only personnel with a valid need-to-know and proper security clearance are allowed access to the system
- Ensure only personnel that have received initial user training and have signed a Classified Information System User Agreement are permitted access to the system
- Maintain a list of authorized users and training records
- Formally notify the ISSO when a system is no longer required to process classified information

6. System Administrator

The System Administrator is responsible for configuring, administering, and maintaining classified information systems. The System Administrator shall possess a clearance equal to or higher than the highest classification of data stored or processed on systems administered. The System Administrator shall:

- Maintain separation of duties by protecting the System Administrator account access rights from the System Owner and all other Users
- Use system administration rights only to perform authorized administrator tasks and functions
- Implement and maintain the technical controls and configuration guidance listed in the SSAA

- Notify the System Owner and the ISSO of any configuration changes that might adversely impact security features
- Maintain configuration management documentation for hardware and software upgrades
- Maintain software licenses and documentation
- Complete the Initial User Training before accessing a system
- Acknowledge, in writing, responsibilities for adequately protecting classified systems
- Complete Annual Refresher Training

7. User

A User can input or modify data on a classified information system. A User shall possess a clearance equal to or higher than the highest classification of data stored or processed on the classified systems authorized by the System Owner to use. The User shall:

- Comply with the requirements of the SSAA
- Be aware of and knowledgeable of responsibilities regarding classified system security
- Be accountable for his/her actions while using the classified information system
- Ensure user password is protected at the highest classification level of data on the system
- Complete the Initial User Training before accessing a system
- Acknowledge, in writing, responsibilities for adequately protecting classified systems
- Complete Annual Refresher Training

Section 3: National Security Systems Identification and Planning

10-300 Identifying Information Systems as National Security Systems

1. A National Security System, as defined by the “Guide for Identification of Information Systems as National Security Systems” (NIST SP 800-59) is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency the function, operation, or use of which:
 - Involves intelligence activities
 - Involves cryptologic activities related to national security
 - Involves command and control of military forces
 - Involves equipment that is an integral part of a weapon or weapons system
 - Is critical to the direct fulfillment of military or intelligence missions
 - Is protected at all times by procedures established for information that have 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

2. If there is a dispute regarding security classification of information processed by a system, the dispute shall be submitted, in writing, to SMD. The DAA and NSI Program Team shall act as arbitrator. If the dispute cannot be resolved internally, or if a dispute involves more than one agency, the issue may be submitted to the Information Security Oversight Office (ISOO) for resolution. If ISOO support is required contact will be initiated, in writing, through the Director, SMD at Information Security Oversight Office, National Archives and Record Administration, 700 Pennsylvania Ave, NW, Room 500, Washington, DC 20408.

10-301 Classified Information Security Planning Standards

1. Major Classified Applications and General Classified Support Systems
 - **Certification and Accreditation**
 - The National Information Assurance Certification and Accreditation Process (NIACAP) described in the National Security and Telecommunications Information System Security Instruction No. 1000 (NSTISSI No. 1000) shall be used for the certification and accreditation process
 - **System Security Authorization Agreements (SSAA)**
 - The SSAA, as required by the NIACAP, shall be used to establish an evolving, yet binding, agreement on the level of security required before the system development begins, or changes are made to a classified system
 - The SSAA, approved by the DAA, is used to guide and document the results of certification and accreditation
 - After accreditation, the SSAA becomes the baseline security configuration document
2. Stand-Alone (Desktop or Laptop) Classified Systems
 - **Registration and Certification Process**
 - Effective security measures used with classified stand-alone systems shall include physical, procedural, and personnel access controls to prevent unauthorized individuals from accessing the systems
 - The approved EPA SSAA Master Plan establishes system-level security requirements, defines operational and technical controls, and establishes access requirements for stand-alone information systems used to process routine office administrative functions (e.g., Microsoft Office applications)
 - The SSAA Master Plan, maintained by the NSI Program Team, further defines the registration and certification process

Section 4: Training

10-400 Security Training Requirements

Security training is an essential aspect of the National Security Systems Program. Users of classified systems will complete Initial User Training prior to being authorized access. Annual Refresher Training is also required for all users. Training materials are developed and maintained by the NSI Program Team.

- **Initial User Training**
 - All users will be trained on security responsibilities prior to being allowed access to classified systems
 - Training will be conducted by the ISSO/ISSR or the NSI Program Team
 - Each individual will receive a Classified System Initial User Training certificate to verify completion of training
 - A copy of the training certificate will be maintained by the System Owner
- **Annual Refresher Training**
 - At a minimum, refresher training shall occur annually, or when there is a change to the security procedures for which a user is responsible
 - Training will be conducted by the ISSO/ISSR or the NSI Program Team
 - Any user not participating in required training shall have user logon rights removed until training is complete

Section 5: Classified Processing Standards

10-500 Personnel Security

The personnel security aspects of classified systems require that an individual's personal reliability and trustworthiness meet specified criteria, and identification of a valid need-to-know to access particular types of data.

1. Security Clearances All personnel approving, certifying, or accessing EPA classified systems must have the following:
 - A security clearance equal to or higher than the highest classification of data stored or processed on the system
 - A valid need-to-know
2. Contract Management Contracting Officer Representatives (COR) must ensure the requirements of this chapter are included in the Contract Security Classification Specification (DD Form 254) for all contractors authorized to process information on EPA classified systems.
3. Visitors Visitors, custodial, and facility maintenance personnel who are inside areas authorized to process classified information and do not have security clearances must be escorted and kept under continuous observation by authorized personnel.
4. Inter-Agency Policy The following policies apply when classified processing is performed at EPA facilities by non-agency personnel or when EPA personnel must process classified information at other U.S. Government facilities:
 - When EPA facilities, organizations, personnel, or contractors are hosting U.S. cleared personnel not associated with EPA and classified processing on EPA systems is required, the computer security policies and procedures of this Handbook apply.
 - When cleared personnel representing the EPA are processing classified information in U.S. Government facilities not operated by EPA, or on non-EPA systems, the computer security policies and procedures of the host department or agency apply

- If there is a conflict regarding which Agency's computer security policies apply, always use the most restrictive procedures

10-501 Physical Security

The physical security aspects of classified systems are designed to protect hardware, software, and other information system components from damage or loss (including loss due to negligence or intentional misconduct).

1. Secure Areas Classified processing shall take place in an open storage or a secure area that has been accredited in accordance with the standards established in Chapter 5, Section 6.
2. Storage Requirements Users of systems must comply with the following storage requirements for classified hard drives and media: (Approved security container requirements are listed in Chapter 5, Section 5.)
 - If a system has a removable hard drive, the hard drive shall be stored in an approved security container when not in use unless the hard drive is physically located in an accredited open storage area
 - If a system does not have a removable hard drive, the computer shall be stored in an approved security container when not in use unless the computer is physically located in an accredited open storage area
 - Removable media (e.g., floppy disks, CDs) must be stored in an approved security container or an open storage area when not in use
3. Document Marking Requirements All documents residing on, printed by, or processed on classified systems or removable storage media will be marked in accordance with the requirements listed in Chapter 4.
4. Media Marking Requirements All hard drives and data storage media will be physically labeled to indicate its security classification. This marking label will reflect the highest security classification level of any information ever stored or processed on the media. When marking media, the standard form labels described in Chapter 4, Section 508 are preferred. If the label impedes operation of the media, a permanent marking on the media may be more appropriate. Media may never be downgraded in classification without approval of the ISSO.
5. Hardware Labeling Requirements Labels shall be displayed on all hardware components of systems that have the potential for retaining information (e.g., monitors, printers, desktops, laptops). The labels should be the same as described above. If the label impedes operation of the component, permanent markings on the component or a sign placed on the terminal is appropriate.

6. Protecting Displayed Information All users must ensure that classified information is not displayed on a monitor when unauthorized individuals are in a position to view the screen. Monitors must face away from windows and open access areas to prevent casual viewing by unauthorized individuals. Monitor and/or video screens that display classified information must be protected in the same manner as other classified information/equipment.
7. Co-location of Classified and Unclassified Computers The following conditions shall be adhered to when a classified computer is co-located with an unclassified computer:
 - A computer approved for processing unclassified information, in a classified environment, must be clearly marked as an unclassified computer
 - A computer approved for processing unclassified information must be physically separated, at least 1 meter, from any classified computers
 - In accordance with NSTISSAM Tempest/2-95, Classified Computers
 - A computer approved for processing unclassified information must not be connected to any classified computer
 - The modem on an unclassified computer must be disabled if it is in the same room as the classified computer
 - The unclassified computer and its data are subject to random reviews and inspections by the ISSO/ISSR. If classified information is found on an unclassified computer, it shall be reported in accordance with Section 10-300
 - Users shall be provided with co-location policies and procedures by the ISSO/ISSR as part of their required security and awareness training

10-502 Administrative Security

The administrative security aspects of classified systems require documentation of critical security actions to demonstrate compliance.

1. Access Access to a system must be restricted. The level of access granted must limit users to only the information needed to complete their assigned duties. At no time will foreign nationals be given access to an EPA-owned classified system. Access is only allowed when the following conditions are met:
 - System Owner has verified the need-to-know
 - NSI Representative has verified the user possesses an appropriate security clearance
 - User has completed Initial User Training and remains current on Annual Refresher Training
 - User has signed a Classified Systems User Agreement
2. Classified Systems User Agreements The Classified Systems User Agreement is a signed acknowledgement of understanding the responsibility for protecting the system and the classified information it contains and processes. The user will be offered the opportunity to sign the agreement upon completion of Initial User Training. Access to the system will only be granted after the agreement is signed.
3. List of Users The System Owner shall maintain a list of authorized users for each system.

4. Access Identification and Authentication Identification and authentication controls are required to ensure that users have the appropriate clearances and a valid need-to-know for the information on a particular system. Minimum requirements for identification and authentication are provided below. Detailed procedures shall be documented in each SSAA.
 - **Authentication Methods**
 - Authentication methods approved by the DAA may include passwords, tokens, biometrics, smartcards, or similar methods
 - **Access to Authentication Data**
 - Access to authentication data shall be restricted to authorized personnel through the use of encryption and/or file access controls
 - **Authentication at Login**
 - Users shall be required to authenticate their identity during login by supplying their authenticator (Password) in conjunction with their user identification (UserID) prior to the execution of any application or utility on the system
 - **UserID**
 - Each user shall be uniquely identified, and that identity shall be associated with all auditable actions. UserIDs are unclassified and will be immediately disabled and permanently deleted when a user no longer requires access
 - **Protection of Individual Passwords**
 - Passwords shall be protected at a level commensurate with the classification of the information to which they allow access
 - The password generation method (e.g., password length, character set) shall be described in the SSAA
5. Malicious Code Prevention Systems will be monitored for changes that may indicate the presence of a computer virus or other malicious code.
 - **Anti-virus Programs**
 - An anti-virus program that checks for known viruses will be applied on a scheduled basis as prescribed in the applicable SSAA
 - Anti-virus programs include an executable file and a separate data file of virus identifying strings, and shall to be updated as new viruses are identified
 - **Preventive Procedures**
 - Scan all information storage media (i.e., diskettes, compact disks, computer hard drives) and email attachments prior to use on any classified system
 - If the media cannot be virus scanned, it will be considered high risk and will not be used on any system
6. Printing Protection Users must ensure that classified files are not stored in a printer's queue and classified information is not left unattended on the printer.

7. Inventory The System Owner must maintain a complete and up-to-date inventory of all system components and peripheral system devices using the registration/certification form or a systems inventory log. This inventory will also be required to obtain initial approval to operate by the DAA.
8. Transferring Information Special procedures apply for transferring data to a classified processing system.
 - **Transferring Classified Data to an Unclassified System**
 - Data generated on a classified system cannot be transferred to an unclassified system, even if the data itself is unclassified
 - **Transferring Unclassified Data to a Classified System**
 - This procedure is only authorized for transferring data from an unclassified information system to a classified information system
 - The following describes the transfer procedure:
 - a. Obtain new blank media for each transfer
 - b. Mark media according to the same classification level as the classified system
 - c. Copy the unclassified data onto the media
 - d. Insert the media into the classified system, and copy the applicable data
 - e. Properly safeguard or destroy media after use
9. Clearing, Sanitization, Destruction, Declassification The unique physical properties and retentive capabilities of magnetic media and devices require special precautions be taken to safeguard all classified information stored on such media. Additionally, residual classified information and/or data may reside on the media. This section provides the methods and procedures used to clear, sanitize, declassify, and destroy classified magnetic media. Note: CD-ROM disks cannot be cleared or sanitized. All CD-ROM disks shall be forwarded to the NSI Program Team for destruction.
 - **Clearing**
 - Clearing is the process of eradicating the data on the media before reusing it in an environment that provides an acceptable level of protection for the data that was on the media before clearing
 - In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval
 - Clearing procedures are approved by the ISSM
 - All media requiring clearing will be forwarded to the NSI Program Team
 - **Sanitization**
 - Sanitization is the process of removing the data from the media before reusing it in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing
 - In general, laboratory techniques cannot retrieve data that has been sanitized. Sanitization procedures are approved by the ISSM
 - All media requiring sanitization will be forwarded to the NSI Program Team

- **Declassification**
 - Declassification is the final administrative step prior to releasing the device or media from continuous protection
 - Declassification requires sanitization and the removal of all classified labels and markings
 - Declassification allows release of the media from the controlled environment
 - All media requiring declassification will be forwarded to the NSI Program Team
 - **Destruction**
 - Destruction is the process of physically damaging the media so that it is not usable as media and that no known method can retrieve data from it
 - All media and devices requiring destruction shall be sent to the NSI Program Team
10. System Maintenance A computer system is particularly vulnerable to security threats during maintenance activities. The following requirements are necessary for maintaining system security during maintenance:
- **Cleared Maintenance Personnel**
 - Personnel who perform maintenance on systems shall be cleared to the highest classification level of information on the system, unless authorized by the DAA
 - Cleared personnel who perform maintenance or diagnostics on a classified system do not require an escort, unless need-to-know controls must be enforced
 - **Uncleared or Lower Cleared Maintenance Personnel**
 - If appropriately cleared personnel are unavailable to perform maintenance, an uncleared person, or one cleared to a lower level may be used
 - a. In this instance, a fully cleared and technically qualified escort monitors and records that person's activities in a maintenance log
 - Prior to maintenance, the system shall be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured
 - A separate, unclassified copy of the operating system and application software shall be used for all maintenance operations performed
 - **General Maintenance Requirements**
 - A maintenance log shall be maintained by the System Administrator
 - The maintenance log shall include the date, time, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts
 - Maintenance of systems shall be performed on-site whenever possible
 - Equipment repaired off-site requires protection from association with the secure facility or program
 - If computer components are to be removed from the facility for repair, they shall first be sanitized of all classified data and declassified in accordance with ISSM-approved procedures

- The ISSO/ISSR shall approve, in writing, the release of all systems and all parts removed from the system
- Maintenance changes that impact the security of the system shall receive a configuration management review by the ISSR
- After maintenance has been performed, the security features on the system shall be recertified

11. Record Keeping Ultimately, the System Owner must ensure that the official records listed below, where applicable, are maintained in a central file for each system authorized to process classified information:

- List of Authorized Users
- Classified System User Agreements
- Contingency Operation, Disaster Recovery, and Emergency Action Plans
- Copies of Waivers or Exceptions
- System Registration/Certification Documentation
- System Maintenance Logs
- Annual Security Reviews
- System Inventories

12. Security Reviews The System Owner, in conjunction with the System Administrator, must conduct an annual self-inspection in accordance with the approved SSAA. The results of the self-inspection review must be retained with the System Administrator and a copy forwarded to the NSI Program Team by September 30th of each year.

10-503 Technical Security

The technical security aspects of classified systems require implementation of methodologies to ensure that data is accessible, verifiable, and secure from unauthorized access or damage. In order to be accredited, each classified system must conform to a set of technical protection measures for confidentiality, integrity, and availability. This section describes measures designed to assist those involved in system development, implementation, certification, and accreditation. To determine which of these requirements are appropriate for a given system, the DAA and System Owner must first ascertain the appropriate Levels-of-Concern and Protection Level.

1. Levels-of-Concern The following describes the three Levels-of-Concern for National Security Systems:

- **Confidentiality**
 - This rating is based on the sensitivity of the information that the system maintains, processes, and transmits; the more sensitive the information, the higher the Level-of-Concern for Confidentiality
 - National Security Systems that process classified information within the EPA will always be assigned a “High” Level-of-Concern
- **Integrity**
 - This rating is based on the degree of resistance to unauthorized modification of the information maintained, processed, and transmitted by the system, necessary for accomplishing the mission of its users

- The greater the needed degree of resistance to unauthorized modification, the higher the Level-of-Concern for Integrity
- **Availability**
 - This rating is based on the degree of ready availability required for information maintained, processed, and transmitted by the system in order to accomplish the mission of its users
 - The greater the need for immediate availability of information, the higher the Level-of-Concern for Availability

2. Determining Levels-of-Concern The Levels-of-Concern Matrix, Table 1, should be used as follows:

- A determination of high, medium, or basic shall be made for each of the three attributes: confidentiality, integrity, and availability
- It is not necessary for the Levels-of-Concern to be the same for all attributes of the system
- When multiple applications on a system result in different Levels-of-Concern for the categories of confidentiality, integrity and availability, the highest level of concern for each category shall be used
- The decision regarding the Levels-of-Concern shall be explicit for all (including interconnected) systems
- A record of this decision shall be documented in the SSAA

Level of Concern	Confidentiality Indicators	Integrity Indicators	Availability Indicators
High	Top Secret Secret Confidential	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.	Information must always be available upon request, with "no" tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	N/A	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.	Information must be readily available with minimum (seconds or hours) tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Basic	N/A	Reasonable degree of accuracy required for mission accomplishment.	Information must be available with flexible tolerance for delay (days to weeks).

Table 1 - Levels-of-Concern Matrix

3. Protection Levels The concept of Protection Levels apply only to the confidentiality Level-of-Concern. The protection level of a system is determined by the relationship between the clearance levels, formal access approvals, need-to-know of users, and the Level-of-Concern. The following provides a description of each Protection Level.

- **Protection Level 1**
 - Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system
 - This means that all users have all required clearances, formal access approvals, and a valid need-to-know for all information on the system (i.e., dedicated mode)
 - **Protection Level 2**
 - Systems are operating at Protection Level 2 when all users have all required clearances, and all required formal access approvals, but at least one user lacks a valid need-to-know for some of the information on the system (i.e., system high mode)
 - **Protection Level 3**
 - Systems are operating at Protection Level 3 when all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system (i.e., compartmented mode)
4. Determining Protection Levels The DAA and the System Owner must assign a Protection Level to each system that is to be accredited. Table 2 presents the criteria for determining which of the three Protection Levels is appropriate for the system being accredited. A record of this decision shall be documented in the SSAA.

Protection Level	Lowest Clearance	Formal Access Approval	Need-to-Know	Level of Concern
PL 1	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	High, Med, Basic
PL 2	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	High, Med, Basic
PL 3	At Least Equal to Highest Data	NOT ALL Users Have ALL	Not contributing to the decision	High, Med, Basic

Table 2 - Protection Level Table for Confidentiality

5. Security Features and Assurances After assigning the Levels-of-Concern and Protection Level described above, the DAA and System Owner shall determine the specific technical security features and their associated assurances for confidentiality, integrity, and availability. In order to be certified and accredited, each system must conform to the set of technical security features associated with the selected Protection Level for confidentiality and Levels-of-Concern for integrity, and availability.

6. Security Features and Assurance Matrix The specific technical security features and associated assurances which a system must comply with are provided in Table 3 (Confidentiality), Table 4 (Integrity), and Table 5 (Availability). Each table is independent of each other. For each Level-of-Concern, follow the appropriate instruction below:
 - **Confidentiality**
 - Find the column representing the Protection Level assigned for confidentiality (e.g., PL1, PL2, PL3) in Table 10-3
 - The cells in the column directly below the Protection Level are the assurance requirements for the associated technical security feature identified in the associated left column
 - A detailed description of each technical security feature is provided in Appendix K
 - **Integrity**
 - Find the column representing the Level-of-Concern for integrity (e.g., Basic, Medium, High)
 - The cells in the column directly below the Levels-of-Concern are the assurance requirements for the associated technical security feature identified in the associated left column
 - A detailed description of each technical security feature is provided in Appendix K

- **Availability**
 - Find the column representing the Level-of-Concern for availability (e.g., Basic, Medium, High)
 - The cells in the column directly below the Levels-of-Concern are the assurance requirements for the associated technical security feature identified in the associated left column
 - A detailed description of each technical security feature is provided in Appendix K

CONFIDENTIALITY			
Technical Security Features	Protection Level Level of Concern (High, Med, Basic)		
	PL 1	PL 2	PL 3
Access Control [Access 1]	X	X	X
Access Control [Access 2]		X	X
Access Control [Access 3]			X
Account Management Procedures [AcctMan]	As Required	X	X
Auditing Procedures [Audit 1]	As Required	X	X
Auditing Procedures [Audit 2]		X	X
Auditing Procedures [Audit 3]		As Required	X
Auditing Procedures [Audit 4]			X
Data Transmission [DataTrans]	X	X	X
Identification & Authentication [I&A 1]	X		
Identification & Authentication [I&A 2]	As Required	X	X
Identification & Authentication [I&A 3]	As Required	X	
Identification & Authentication [I&A 4]		X	X
Identification & Authentication [I&A 5]			X
Least Privilege [LeastPrv]		X	X
Resource Control [ResrcCtrl]		X	X
Security Documentation [Doc 1]	X	X	X
Security Documentation [Doc 2]		X	X
Security Documentation [Doc 3]		As Required	X
Security Testing [Test 1]	X		
Security Testing [Test 2]		X	X
Security Testing [Test 3]		As Required	X
Separation of Functions [Separation]	X	X	X
Session Control [SessCtrl 1]	X	X	X
Session Control [SessCtrl 2]		X	X
System Recovery [Recovery]	X	X	X

Table 3 - Security Features and Assurances Matrix for Confidentiality

INTEGRITY			
	Level of Concern		
Technical Security Features	Basic	Medium	High
Backup Procedures [Backup 1]	X	X	X
Backup Procedures [Backup 2]		X	X
Backup Procedures [Backup 3]			X
Change Control [Change 1]		X	X
Change Control [Change 2]			X
Malicious Code [MalCode]	X	X	X
System Assurance [SysAssur 1]		X	X
System Assurance [SysAssur 1]			X

Table 4 - Security Features and Assurances Matrix for Integrity

AVAILABILITY			
	Level of Concern		
Technical Security Features	Basic	Medium	High
Backup Procedures [Backup 1]	X	X	X
Backup Procedures [Backup 2]		X	X
Backup Procedures [Backup 3]			X
Backup Power [Power 1]	As Required	X	X
Backup Power [Power 2]		As Required	X

Table 5 - Security Features and Assurances Matrix for Availability

Chapter 11: SPECIAL ACCESS PROGRAMS

Section 1: Overview

11-100 Overview

Special Access Programs (SAP) have been established to impose access, storage, and handling controls beyond those normally required for access to information classified as Confidential, Secret, or Top Secret. These programs require special clearances, special investigative requirements, and special briefings. This chapter covers EPA's Sensitive Compartmented Information (SCI) Program, a SAP, and describes the program's policies and procedures.

Section 2: Special Access Programs

11-200 Policy

1. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and the Director, Central Intelligence Agency may create a SAP.
2. The granting of access to SAPs will be controlled under the strictest application of the need-to-know principle, in accordance with the personnel security standards and specific procedures set forth by the programs.
3. The NSI Program Team supports the administrative needs of EPA federal and non-federal employees requiring authorization for access to a SAP.

Section 3: Sensitive Compartmented Information (SCI) Program

11-300 Authority

1. EPA employees granted access to SCI shall comply with policies established by this chapter, in addition to applicable Executive Orders (E.O.), directives, and regulations.
2. United States intelligence activities are governed by E.O. 12333, which establishes the Intelligence Community and provides the Director of Central Intelligence with the responsibility to protect intelligence sources, methods, and analytical procedures.
3. Security policies for SCI are documented in Director of Central Intelligence Directives (DCID). The following is a list of DCIDs that SCI-cleared EPA employees will most often utilize. A complete listing of DCIDs can be obtained from the NSI Program Team.
 - DCID 1/19 - Security Policy for Sensitive Compartmented Information, dated March 1, 1995
 - DCID 6/3 - Protecting SCI within Information Systems Manual, dated June 5, 1999
 - DCID 6/4 - Personnel Security Standards and Procedures Governing Eligibility for Access to SCI, dated July 2, 1998

- DCID 6/9 - Physical Security Standards for SCI Facilities, dated November 18, 2002

11-301 SCI Program Management

The National Security Act of 1947 established the National Foreign Intelligence Programs (NFIP). The NFIP was re-designated to the National Intelligence Programs (NIP) in 2004 by the Intelligence Reform and Terrorism Prevention Act. The National Intelligence Board (NIB), formally the National Foreign Intelligence Board, established by E.O. 12333, serves as senior Intelligence Community advisors to the Director of National Intelligence. The board is composed of senior representatives from organizations within the Intelligence Community that are mainly responsible for the collection, processing, and analysis of intelligence. Because EPA is not a member of the NIB, it is invited to participate when matters in its interest are considered. Non-NIB Agencies fall under the direction and oversight of their sponsoring Agency; therefore, EPA falls under the direct oversight from the Central Intelligence Agency. The roles and responsibilities for EPA's SCI program are as follows:

1. Central Intelligence Agency

- Provide SCI program direction and oversight
- Grant authorization for SCI access
- Maintain a database of all SCI access
- Accredite SCI Facilities (SCIF) for EPA
- Evaluate an individual's continuing eligibility for SCI access
- Ensure all security violations, infractions, compromises, and unauthorized disclosures are properly investigated

2. Office of the Administrator, EPA (AO)

- Responsible for determining if EPA personnel requesting SCI access have a requirement and a valid need-to-know

3. Special Security Officer (SSO)

A federal staff member of the NSI Program Team is designated as EPA's SCI Special Security Officer (SSO). The SSO shall possess SCI accesses for each program handled by EPA. The SSO shall:

- Coordinate with CIA for EPA's SCI program
- Coordinate between AO and EPA personnel
- Conduct SCI program indoctrination briefs and training for EPA personnel
- Initiate SCI access requests for submission to CIA
- Process visit requests for submission to CIA for certification
- Maintain required SCI administrative files
- Conduct periodic reviews of EPA SCIFs
- Administer SCI training and education programs

11-302 SCI Administration

Particular categories of classified intelligence information require special security access, special handling, and special storage facilities not covered by procedures for Confidential, Secret, and Top Secret information. Special procedures are prescribed in directives, regulations, and instructions relating to Sensitive Compartmented Information (SCI). In order to function effectively, EPA's SCI program administration is standardized. The requirements for initial access to SCI include:

1. Obtaining SCI Access To obtain access to SCI programs, personnel shall possess a Top Secret clearance based on a favorable Single Scope Background Investigation (SSBI) or Periodic Review (PR) completed within the last five years. Requests for SCI access are submitted to the NSI Program Team via the SCI Authorization Request Form, provided in Appendix L.
 - The Requestor must initiate an SCI Authorization Form, identify access(es) required, and have an unclassified justification approved by his/her supervisor
 - The NSI Program Team shall review this form to ensure the requestor meets the appropriate investigation and clearance requirements
 - Upon AO's authorization, the NSI Program Team shall forward the special access request(s) to CIA for adjudication
2. Accessing Information Prior to accessing SCI, employees must obtain initial SCI training, program indoctrination briefing(s), and sign the SCI Nondisclosure Agreement, SF 4414.
 - The SCI Nondisclosure Agreement, SF 4414, is a lifetime agreement and is maintained in a personnel file by CIA for 70 years
 - When access is no longer required, due to separation, transfer, change in duties, suspension, or revocation of access, the NSI Program Team will provide SCI security debriefings
 - EPA personnel with questions and/or concerns regarding their accesses should contact the NSI Program Team
3. Visit Certifications In order to utilize SCI access at another agency and/or facility, EPA personnel must have their SCI accesses certified. There are two types of certification: Visit Certification and Permanent Visit Certification. A Visit Certification is used to certify an individual's accesses for a singular (non-recurring) event, while a Permanent Visit Certification is issued for a recurring need to visit another agency and/or facility for the duration up to one year. The following procedures define the requirements for sending and/or receiving Visit Certifications:
 - Sending SCI Visit Certifications
 - Personnel are required to submit the SCI Visit Certification Request Form, provided in Appendix M, to the NSI Program Team at least five working days prior to the intended visit
 - The NSI Program Team will forward a visit certification request to CIA
 - The CIA will officially submit the visit certification to the appropriate agency and/or facility

- The NSI Program Team will verify that the clearances were received by the receiving agency and/or facility
 - The NSI Program Team will track the expiration of Permanent Visit Certifications and inform the original requestor of a pending expiration
 - **Receiving SCI Visit Certifications**
 - Individuals visiting an EPA facility must forward Visit Certifications to the NSI Program Team prior to the visit. (Hand-carried Visit Certifications are not authorized)
 - It is the host's responsibility to verify visitor's SCI access with the NSI Program Team prior to engaging in SCI meetings
 - The host must coordinate with the NSI Program Team to ensure the meeting and/or discussion occurs within an accredited SCIF
4. Reporting Individuals granted SCI access are obligated to report, in writing, any activities, conduct, or employment that may affect their ability to protect classified information from unauthorized disclosure or counter-intelligence threats to the NSI Program Team. A complete list of reporting requirements can be found in DCID 6/4. The NSI Program Team maintains standardized forms for three of the required reporting functions:
- **Foreign Travel Notification**
 - SCI cleared individuals are required to submit this form (10 days prior to departure) to the NSI Program Team, reporting official or unofficial foreign travel
 - **Suspicious Contact Questionnaire**
 - SCI cleared individuals are required to submit this form to the NSI Program Team, reporting any contact with individuals (foreign or domestic) that are considered threatening or suspicious
 - **Continuous Foreign Contact**
 - SCI cleared individuals are required to submit this form to the NSI Program Team, reporting close and continuing contact with foreign nationals
5. SCI Control and Accountability Controls are procedures used to provide a degree of physical protection necessary to safeguard, handle, and manage SCI. Accountability is an application of control; it provides a formal mechanism to maintain a constant level of accountability for SCI. EPA accounts for all Top Secret information, including Top Secret SCI.
- Top Secret SCI Accountability
 - All Top Secret SCI (including copies) originated or received by an office shall be continuously accounted for, individually serialized, and entered into the SSO's Top Secret SCI log
 - The log shall include the date originated or received, individual serial number, copy number, title (unclassified if possible), originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified), and date of each disposition

- Top Secret SCI shall be inventoried annually (with the results compiled by September 30), at the change of the SSO, and/or upon the report of loss or compromise
 - a. One complete copy of the Top Secret SCI inventory will be forwarded to the NSI Program Team
 - During the annual inventory, each document must be visually inspected to determine possible downgrade, declassification, or required destruction
 - The Classified Information Accountability Record, provided in Appendix H, shall be used to record transmission, reproduction, and destruction of Top Secret SCI and shall be maintained for five years
 - Secret and Confidential Control
 - Stringent control measures shall be in place for Secret and Confidential SCI
 - Each document must be visually inspected to determine possible downgrade, declassification, or destruction of classified holdings to reduce the amount necessary for operational and program purposes
 - Control measures include external receipts and dispatch records to ensure that documents are tracked during transmission
 - a. The Classified Information Accountability Record, provided in Appendix H, shall be used as a record of receipt and shall be maintained for two years
6. SCI Transmission SCI transmissions shall be accomplished in a manner to preclude loss or compromise. While transmitting SCI, it must be controlled through authorized transmission methods, and accounted for by use of a Classified Information Accountability Record, provided in Appendix H. Under no circumstances will SCI be transmitted via the U.S. Postal Service or other commercial courier services.
- The authorized methods are:
 - Direct contact between authorized persons
 - Defense Courier Service (DCS)
 - Department of State Diplomatic Courier System
 - Designated courier with appropriate SCI access
 - Electronic means over SCI approved communications systems

11-303 Infractions, Violations, Compromises, and Unauthorized Disclosures

Any employee with knowledge of any possible or actual security violations, infractions, or compromise involving SCI shall utilize the procedures established in Chapter 1, Section 3. If the Director, SMD determines that an incident is a significant security violation or compromise, as defined by DCID 6/8, CIA shall be immediately notified.

11-304 SCI Facilities (SCIF)

SCI information must be safeguarded in a more stringent manner than that of collateral Confidential, Secret, and Top Secret information. SCI may only be stored, used, discussed, and/or electronically processed/transmitted within an accredited SCIF. A SCIF is an accredited area, room, or group of rooms intended to prevent visual, acoustical, technical, and physical access by unauthorized persons. Accreditation is the

formal approval acknowledging that a facility meets prescribed physical, technical, and personnel security standards. SCIF standards are outlined in DCID 6/9.

1. Obtaining an Accredited SCIF To obtain an accredited SCIF:
 - Provide written justification to the NSI Program Team for review
 - Upon approval of justification, submit an accreditation package to the NSI Program Team containing the following:
 - Fixed Facility Checklist (DCID 6/9, Appendix A)
 - Floor plans
 - Diagrams of electrical communications
 - Heating, ventilation, air conditioning (HVAC) connections
 - Security equipment layout (to include the location of intrusion detection equipment)
 - Any other applicable documentation, as required
 - The NSI Team will review the completed package, and coordinate accreditation activities with CIA
 - Upon approval of the facility, CIA shall provide the official accreditation letter
 - The original official accreditation letter shall be maintained within the SCIF, and an additional copy shall be maintained by the NSI Program Team

2. SCIF Administrative Requirements All SCIFs must maintain the following:
 - Approved DCID 6/9 Fixed Facility Checklist
 - Official accreditation letter
 - Inspection reports for the entire period of SCIF accreditation
 - Operating procedures, Special Security Officer appointment letters, Memorandum of Agreement (MOAs), and Emergency Action Plans
 - Copies of any accreditation waivers granted by CIA
 - Records for personnel access control shall reflect the current active assignment of ID badge/card, PIN, level of access, entries, and similar system-related elements
 - Records concerning personnel removed from the system shall be retained for a minimum of two years
 - Records of entries to SCIFs shall be retained for a minimum of two years or until investigations of system violations and incidents have been successfully resolved and recorded
 - Procedures for identification and control of visitors to the SCIF
 - Security Container Information Form (SF 700)
 - Activity Security Checklist (SF 701)
 - Security Container Check Sheet (SF 702)
 - Visitor log
 - All persons not assigned to the facility shall log in regardless of their clearance level
 - The log shall include the visitors' full name, SSN, purpose of visit, date of visit, signature/printed name of the escort, and the time entered/departed

3. Withdrawal of SCIF Accreditation When a SCIF is no longer required, the NSI Program Team shall be notified to conduct a close out inspection. The purpose is to ensure that all SCI information has been removed from the facility. Upon completion of the final inspection, the NSI Program Team shall provide the CIA with a letter certifying the SCIF's withdrawal.

11-305 Contracts Requiring SCI Access

Contract Officer Representatives must ensure that contractors requiring SCI access have incorporated/referenced the requirements established in this chapter within each Contract Security Classification Specification (DD 254).

11-306 SCI Security Education

The NSI Program Team shall administer a continuing security education program for all personnel authorized access to Sensitive Compartmented Information. Under the program, individuals with SCI access shall be reminded of their obligation to properly handle and safeguard SCI information and of the potential consequences to the U.S. Government of any compromise or unauthorized use of such information. This training program shall include:

1. Initial Indoctrination This training is administered with a non-SCI-revealing briefing followed by a program specific briefing.
 - Non-SCI-Revealing Brief
 - This brief, designed to provide an introduction to the general nature of SCI and its safeguarding requirements, is to be administered prior to initial access to SCI
 - Upon completion of training, each individual is offered the opportunity to sign the SCI Nondisclosure Agreement (SF 4414)
 - a. Individuals unwilling to sign the SCI Nondisclosure Agreement shall not be granted SCI access
 - b. Subsequent to signing the SF 4414, individuals shall be fully indoctrinated on the aspects of SCI which they are authorized access
 - Program Specific Briefing
 - This brief describes the compartments to which access has been granted
 - The indoctrination will be structured to inform recipients of the sensitivity of the information and appropriate cautions concerning answers to questions from non-briefed persons (i.e., family, personal associates, media and journalists)
 - SCI Indoctrination Briefing
 - This brief describes:
 - a. Personal, administrative, and procedural requirements that recipients will be expected follow while they are granted continued access to SCI
 - b. Criminal and administrative sanctions that may be imposed for security violations
 - c. Techniques employed by foreign intelligence organizations in attempting to obtain national security information

2. Refresher Training The training, designed to provide a review of SCI security policy, procedures, and administrative requirements.
 - Conducted annually, at a minimum, by the NSI Program Team to all SCI-cleared individuals
 - A record of training shall be maintained by the NSI Program Team
3. Defensive Travel Briefing This briefing is designed to provide awareness of security vulnerabilities and personal responsibilities associated with foreign travel.
 - This training is to be administered prior to official and unofficial foreign travel to any individual possessing SCI access
4. Security Access Debriefing The briefing shall serve as a reminder to personnel of their continuing obligation to safeguard all SCI information.
 - Administered whenever access is no longer required, due to separation, transfer, change in duties, suspension, or revocation of access
 - At the conclusion of the briefing, personnel will be asked to sign the debriefing section of the SCI Nondisclosure Agreement
5. Emergency Plan Training and Exercises All personnel shall be made aware of the emergency plans through training and exercises. Exercises shall be conducted as circumstances warrant, but no less frequently than annually. Emergency training and exercises shall be reviewed annually and updated as necessary.

11-307 Technical Requirements

Effective security measures used with SCI information systems shall include stringent physical, procedural, and personnel access controls to prevent unauthorized individuals from accessing the systems. Policy, standards, and procedures for certification and accreditation of SCI systems are located in DCID 6/3.

- The certification and accreditation process includes the approval of a System Security Plan (SSP) as defined in DCID 6/3 (Appendix C). The System Owner is responsible for writing the SSP
- The NSI Program Team shall:
 - Provide review and assistance with the development of the SSP
 - Coordinate with the appropriate Designated Accrediting Authority

Appendix A DEFINITIONS

This page is intentionally blank

Definitions

Access - Ability or opportunity to gain knowledge of classified information.

Authorized Person - A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

Automated Information System - An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

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 E.O.12958, as amended.

Classification - The act or process by which information is determined to be classified.

Classified Contract - Any contract that requires, or will require, access to classified information by a contractor or his/her employees on the performance of the contract. A contract may be classified even though the contract document is not classified. The requirements prescribed for classified contracts are also applicable to all phases of contract activity that require access to classified information.

Classification Guidance - Any instruction or source that prescribes the classification of specific information.

Classification Guide - 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 National Security Information or Classified Information - Information that has been determined pursuant to E.O. 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure, and is marked to indicate its classified status when in documentary form.

Classified Visit - A visit during which the visitor will require, or is expected to require, access to classified information.

Cleared Commercial Carrier - A carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL information and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

Collateral Information – Information identified as National Security Information under the provisions of E.O. 12958, as amended, but not subject to enhanced security protection required for Special Access Program Information.

Cognizant Security Agency (CSA) - Agencies of the Executive Branch that have been authorized, by E.O. 12829, to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry.

Compromise - An unauthorized disclosure of classified information.

Contractor - Any industrial, educational, commercial, or other entity that has been granted a Facility Security Clearance (FCL) by a cognizant security agency (CSA).

Contract Security Classification Specification (DD Form 254) - The DD 254, with any attachments or incorporated references, is the legally binding exhibit of a federal contract. It is the only authorized vehicles for conveying to a contractor the security classification guidance for classified national security information.

Control - The authority of the agency that originates information, or its successor in function, to regulate access to the information.

Damage To National Security - Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassified or Declassification - The authorized change in the status of information from classified information to unclassified information.

Declassification Authority - (1) The official who authorized the original classification, if that official is still serving in the same position; (2) the originator's current successor in function; (3) a supervisory official of either; or (4) officials delegated declassification authority in writing by the Agency head or the Senior Agency Official.

Declassification Guide - Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Derivative Classification - Incorporating, paraphrasing, restating, or generating, in new form, information that is already classified, and marking the newly developed information consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance or guides. The duplication or reproduction of existing classified information is not derivative classification.

Document – Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual material and electromagnetic storage media.

Downgrading - A determination by the OCA or a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Facility Security Clearance (FCL) - 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).

Federal Record - Includes all books, papers, maps, photographs, machine-readable information, or other documentary information, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriated for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum information made or acquired and preserved solely for reference, and stocks of publications and processed documents are not included. (44 U.S.C. 3301)

File Series - A body of related records created or maintained by an agency, activity, office or individual. The records may be related by subject, topic, form, function, or filing scheme. An agency, activity, office, or individual may create or maintain several different file series, each serving a different function. Examples may include a chronological file or a record set of agency publication. File series frequently correspond to items on a NARA-approved agency records schedule.

Foreign Government - Any national governing body organized and existing under the laws of any country, other than the United States and its possessions and trust territories, and any agent or instrumentality of that government.

Foreign Government Information - (1) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the United States Government pursuant to or as a result of a combined arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as "foreign government information" under the terms of a predecessor order to E.O. 12958.

Information - Any knowledge that can be communicated or documentary information, 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. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Infraction - Any unintentional action contrary to the requirements of E.O. 12958 or its implementing directives that does not constitute a violation.

Integrity - The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Mandatory Declassification Review - The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of E.O.12958.

Multiple Sources - Two or more source documents, classification guides, or a combination of both.

National Industrial Security Program Operating Manual (NISPOM) - This manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. The manual also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal regulations.

National Security - The national defense or foreign relations of the United States.

Need-To-Know - A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Network - A system of two or more computers that can exchange data or information.

Non-Federal Employees - Contractors, licensees, certificate holders, or grantees

Open Storage Accredited Area - An area constructed in accordance with Chapter 5, Section 5 and authorized in writing for open storage of classified information.

Original Classification - An 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, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

Permanent Records - Any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent of SF 115s, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973.

Personnel Security Clearance (PCL) - 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 PCL being granted.

Records - The records of an agency and Presidential papers or Presidential records, as those terms that are defined in Title 44 United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

Records Having Permanent Historical Value - Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with Title 44 United States Code.

Redaction - The removal of exempted information from copies of a document.

Regrade - To raise or lower the classification assigned to an item of information.

Safeguarding - Measures and controls that are prescribed to protect classified information.

Security Clearance - Determination that a person is eligible, under the standards of E.O. 12968, to access to classified information.

Security-In-Depth - A determination by the accrediting official that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to use of perimeter fences, employee and visitor access controls, use of an IDS, random guard patrols during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

Self-Inspection - The internal review and evaluation of individual agency activities and the agency as a whole, with respect to the implementation of the program established under E.O. 12958 and its implementing directives.

Senior Agency Official - The official designated by the agency head under section 5.4(d) of E.O. 12958, as amended, to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Source Document - An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Systematic Declassification Review - The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with Title 44 United States Code.

Telecommunications - The preparation, transmission, or communication of information by electronic means.

Unauthorized Disclosure - A communication or physical transfer of classified information to an unauthorized recipient.

Violation - (1) Any knowing, willful, or unknowing action that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) any knowing, willful, or unknowing action to classify or continue the classification of information contrary to the requirements of this handbook or its implementing directives; or (3) any knowing, willful, or unknowing action to create or continue a special access program contrary to the requirements of this handbook.

Appendix B PRELIMINARY INQUIRY REPORT

This page is intentionally blank

Preliminary Inquiry Report

(Date)

From: (Name of individual conducting the Preliminary Inquiry)

To: Environmental Protection Agency
Security Management Division
Attn: NSI Program Team
1200 Pennsylvania Ave., NW
Mail Code 3206R Room G.1-1
Washington, DC 20460

Subj: PRELIMINARY INQUIRY (PI)

Ref: (a) EPA NSI Handbook
(b) (if any)

Encl: (1) (if any)

1. Type of Incident: (Loss or compromise)
2. Incident Description: (When, where, and how did the incident occur?)
3. Statement of Facts: (What specific classified information was involved? Keep unclassified if possible. If not, find a stand-alone classified computer to process this report.)
 - a. Identification of lost or compromised information or equipment.

- (1) Classification: (include warning notices/intelligence control markings)
- (2) Identification/Serial Number(s):
- (3) Date:
- (4) Originator:
- (5) OCA(s):
- (6) Subject or Title:
- (7) Downgrading/Declassification Instructions:
- (8) Number of pages or items of equipment involved:
- (9) Point of contact and phone number:
- (10) Custodial program or facility:

4. Assessment of likelihood of loss or compromise: (Assess whether there was an actual or potential loss or compromise of classified information. Was there a failure to comply with established security practices and procedures that could lead to loss or compromise if left uncorrected?)

5. Circumstances surrounding the incident: (Provide an explanation of the contributing factors. What steps were taken to locate the information? How long had the information been missing? Was the material properly classified, stored, and accounted for?)

6. Individual(s) responsible: (What person(s) caused or contributed to the incident?)

7. Identification of security weakness or vulnerability: (Which situations or conditions caused or contributed to the incident? Was there a weakness or vulnerability in established security practices and procedures that might result in a compromise if left uncorrected?)

8. Conclusion: (Choose one of the following statements that best describes the severity of the incident.)

a. A loss or compromise of classified information did not occur, but the action meets the criteria of a security incident;

b. A loss or compromise of classified information did not occur; however, security weakness or vulnerability was revealed due to the failure of person(s) to comply with established security regulations;

c. A loss or compromise of classified information may have occurred but the probability of compromise is remote and the threat to the national security minimal;

d. A loss or compromise of classified information may have occurred due to a significant security weakness or vulnerability; or

e. A loss or compromise of classified information occurred, and the probability of damage the national security cannot be assessed until completion of further investigation.

9. Steps taken: (List the steps taken to date to correct the situation.)

Appendix C ANNUAL NSI DATA COLLECTION REPORT

This page is intentionally blank

Annual NSI Data Collection Report

Submission of this form is to be received no later than September 30 of the current fiscal year by the NSI Program Team. To expedite the process of submission, please fax the form to: 202-565-2028
ATTN: NSI Program Team

Section A: Identifying Information

1. Fiscal Year

2. Area Location Information

EPA Region:
Organization Name:
Program Name:

3. Responsible NSI Representative

NSI Representative:
Work Phone:
Fax Number:
Secure Phone:
Secure Fax Number:

Section B: Original Classification Decisions

Original classification is an initial determination that the information to be classified that has not **been previously classified** by any other authority. It also meets the following conditions: 1) It was classified by an original classification authority; 2) The information is owned by, produced by or for, or is under the control of the United States Government; 3) It falls into at least one of the categories found in Section 1.4 of E.O. 12958, as amended, and; 4) Unauthorized disclosure could be expected to result in damage to the national security. [Provide information only on classification decisions contained in **finished products** for dissemination or retention, **regardless of the media**. Do not count reproductions or copies.]

1. Enter the number of original SECRET classification decisions made during the reporting period with declassification instructions of 10 years or less.

1.

2. Enter the number of original SECRET classification decisions made during the reporting period with declassification instructions ranging from over 10 years to 25 years.

2.

3. Total number of SECRET original classification decisions (Sum of blocks 1 & 2).

3.

4. Enter the number of original CONFIDENTIAL classification decisions made during the reporting period with declassification instructions of 10 years or less.

4.

5. Enter the number of original CONFIDENTIAL classification decisions made during the reporting period with declassification instructions ranging from over 10 years to 25 years.

5.

6. Total number of CONFIDENTIAL original classification decisions (Sum of blocks 4 & 5).

6.

7. Total number of original classification decisions (Sum of blocks 3 & 6).

7.

Section C: Derivative Classification Decisions

Derivative classification is incorporating, paraphrasing, restating, or generating, in new form, information that is **already classified**. This includes classification based on classification guides or other source documents. If possible, include derivative classification actions made by contractors.

1. Enter the number of derivative TOP SECRET classifications during the reporting period.

1.

2. Enter the number of derivative SECRET classifications during the reporting period

2.

3. Enter the number of derivative CONFIDENTIAL classifications during the reporting period

3.

4. Total number of derivative classifications during the reporting period

4.

This page is intentionally blank

Appendix D SELF-INSPECTION CHECKLIST

This page is intentionally blank

Self-Inspection Checklist

Yes No N/A

NSI Management

- | | | | |
|-------|-------|-------|---|
| _____ | _____ | _____ | 1. Does the senior management provide the necessary resources for effective implementation for the NSI Program? |
| _____ | _____ | _____ | 2. Have primary and alternate NSI Representatives been assigned in writing? |
| _____ | _____ | _____ | 3. Does the NSI Representative maintain up-to-date copies of appropriate orders, directives, manuals, handbooks and guides? |
| _____ | _____ | _____ | 4. Does the NSI Representative develop and maintain local SOPs for his/her NSI related activities? |
| _____ | _____ | _____ | 5. Are local SOPs part of the security orientation for assigned personnel with clearances? |
| _____ | _____ | _____ | 6. Do producers and users of classified information receive guidance with respect to security responsibilities and requirements? |
| _____ | _____ | _____ | 7. Does the NSI Representative conduct an annual self-inspection on his/her area of responsibility and submit it to the NSI program team? |

Security Incidents and Reporting Requirements

- | | | | |
|-------|-------|-------|--|
| _____ | _____ | _____ | 8. Do the users of classified information understand the reporting requirements for an actual or possible loss of classified information? |
| _____ | _____ | _____ | 9. Since the last self assessment, has the program or facility had any incidents involving a loss or compromise of classified information? |
| _____ | _____ | _____ | 10. If yes, was the security incident reported to EPA security officials as required? |
| _____ | _____ | _____ | 11. Are Preliminary Inquiries conducted for each incident? |
| _____ | _____ | _____ | 12. Are protective measures taken to preclude recurrence? |
| _____ | _____ | _____ | 13. Are lessons learned included in the security awareness program? |

Classification Management

- | | | | |
|-------|-------|-------|--|
| _____ | _____ | _____ | 14. Does the NSI Representative have a method to track all original and derivative classification decisions in his/her area of responsibility? |
|-------|-------|-------|--|

Yes	No	N/A	
_____	_____	_____	15. Is the Annual NSI Data Collection Report submitted on time (e.g., September 30 of each year)?
_____	_____	_____	16. Do subject matter experts that develop information requiring an original classification decision understand the process to obtain a decision from the OCA?
_____	_____	_____	17. Are documents pending an original classification decision safeguarded in a manner prescribed according to its proposed classification?
_____	_____	_____	18. Are security classification guides developed for each system, plan, program, or project in which classification information is involved?
_____	_____	_____	19. Is each security classification guide approved in writing by an OCA?
_____	_____	_____	20. Are security classification guides reviewed whenever necessary to promote effective derivative classification decisions or, at a minimum, every 5 years?
_____	_____	_____	21. Do local procedures prohibit the use of terms such as "FOUO" or "Secret Sensitive" for the identification of classified NSI?
_____	_____	_____	22. If classification challenges occur, have the proper procedures been followed?
_____	_____	_____	23. Does the derivative classifier maintain a copy of the original source document with the derivatively classified document?
_____	_____	_____	24. Are markings on derivative classified documents consistent with the classification markings on the source information?
_____	_____	_____	25. Does the NSI Representative review all classified documents annually to verify the duration of classification date and remark applicable documents with the new classification?

Classification Markings

_____	_____	_____	26. Are classified documents properly marked to include all applicable markings (e.g., overall, page, and portion markings)?
_____	_____	_____	27. Are originally classified documents marked with a classification block that consists of "Classified by", "Reason", and "Declass on" lines?
_____	_____	_____	28. Are derivatively classified documents marked with a classification block that consists of "Derived from" and "Declass on" lines?
_____	_____	_____	29. Is classified information such as maps, charts, graphs, photographs, slides, recordings, videotapes, and computer media appropriately marked?

Yes	No	N/A	
_____	_____	_____	30. Are working papers dated when created, marked “Working Paper”, and brought under accountability after 180 days or when they are released outside the Agency?
_____	_____	_____	31. Are markings such as “For Official Use Only,” “Sensitive But Unclassified”, “Limited Official Use,” "Law Enforcement Sensitive", or “Sensitive Security Information” used to identify classified national security information?

Safeguarding

_____	_____	_____	32. Before classified information is disclosed, does the holder verify the recipient's security clearance with his/her NSI Representative, determine the recipient's need-to-know, verify the recipient's identification, and advise the recipient of the classification level of the information?
_____	_____	_____	33. Are procedures in place to ensure that visitors have access to only information for which they have a need-to-know and the appropriate clearance level?
_____	_____	_____	34. Are procedures in place for classified meetings to be held within the facility?
_____	_____	_____	35. Is Top Secret information including copies, originated or received by the program or facility, continuously accounted for, individually serialized, and entered into a Top Secret logs?
_____	_____	_____	36. Is Top Secret information accounted for at least annually, at the change of NSI Representatives, and upon report of loss or compromise of information or information?
_____	_____	_____	37. Does the NSI Representative, maintaining Secret or Confidential classified information, conduct an annual review of his/her classified holdings to determine possible downgrade, declassification, or destruction of classified holdings to reduce the amount necessary for operational and program purposes.
_____	_____	_____	38. Are the results of the annual accountability and reviews forwarded to the NSI Program Team?
_____	_____	_____	39. Do all cleared employees who resign, transfer, or retire return all classified information in their possession?
_____	_____	_____	40. Are procedures established for end-of-day security checks, to include the use of SF 701 and SF 702?

Yes	No	N/A	
_____	_____	_____	41. Are classified cover sheets (e.g., SF 703, SF 704, and SF 705) placed on all classified information when removed from secure storage?
_____	_____	_____	42. Are media marking labels (SF 706, SF 707, SF 708, and SF 712) being utilized on all classified AIS media?
_____	_____	_____	43. Are classified typewriter ribbons, carbon sheets, plates, stencils, drafts, and notes controlled, handled, and stored per their classification level?
_____	_____	_____	44. Are necessary copies made on a dedicated classified copy machine?
_____	_____	_____	45. Are signs posted near copy machines indicating the level of classified that may or may not be reproduced on the machine?
_____	_____	_____	46. Is classified information reproduced only to the extent that is essential?

Storage

_____	_____	_____	47. Is classified information stored under conditions that will provide adequate protection and prevent access by unauthorized personnel?
_____	_____	_____	48. Does the security equipment (containers and locks) meet the minimum standards of GSA?
_____	_____	_____	49. Does the NSI Representative ensure that external markings on security containers do not reveal the level of information stored within?
_____	_____	_____	50. Are container combinations changed:
_____	_____	_____	• By individuals who possess the appropriate clearance level?
_____	_____	_____	• Whenever the container is first put into use?
_____	_____	_____	• Whenever an individual knowing the combination no longer requires access to the container (unless other sufficient controls exist to prevent access)?
_____	_____	_____	• Whenever a combination has been subjected to compromise?
_____	_____	_____	• Whenever a container is taken out of service?
_____	_____	_____	51. Are SF 700s utilized to maintain security container information?
_____	_____	_____	52. Are SF 700s properly marked to indicate the level of classification of the combination?
_____	_____	_____	53. Is Attachment 1 of the SF 700 affixed inside each security container?
_____	_____	_____	54. Does the SF 700 include the names, home addresses, and phone numbers of all persons having knowledge of the combination?
_____	_____	_____	55. Does the NSI Representative maintain the record of combinations (e.g., SF 700s) in a separate location protected at the classification level of each combination?

Yes	No	N/A	
_____	_____	_____	56. Are all Open Storage and Secure Areas accredited by the NSI Program Team?
_____	_____	_____	57. Does the NSI Representative maintain a copy of all accreditations?
_____	_____	_____	58. Does the NSI Representative utilize the Accreditation Status Form to communicate accreditation status with the NSI Program Team?

Destruction

_____	_____	_____	59. Are local procedures established for the destruction of classified information?
_____	_____	_____	60. Are reviews conducted periodically to ensure classified information is destroyed when no longer required?
_____	_____	_____	61. Are all classified information shredders NSA-approved crosscut shredders?
_____	_____	_____	62. Are records of Top Secret destruction maintained in the Top Secret accountability files?

Transmission Methods

_____	_____	_____	63. Are classified information receipts used for transferring documents between facilities or agencies?
_____	_____	_____	64. Are receipts for Top Secret information retained for 5 years and receipts for Secret information retained for 2 years?
_____	_____	_____	65. Does the NSI Representative ensure that only appropriately cleared personnel or authorized carriers transmit, transport, escort, or hand-carry classified information?
_____	_____	_____	66. Do cleared employees required to hand-carry classified information have courier cards issued to them?
_____	_____	_____	67. Has the NSI Representative developed local procedures to ensure classified information can be tracked, properly disseminated, and quickly detected if lost?
_____	_____	_____	68. Has the NSI Representative developed and implemented local procedures to protect incoming mail, bulk shipments, and items delivered by messenger containing classified information?
_____	_____	_____	69. Are secure phones installed in appropriately accredited areas?

Yes No N/A

Education and Training

- _____ _____ _____ 70. Have all cleared personnel received initial security orientation training?
- _____ _____ _____ 71. Is specialized training given to the NSI Representatives, subject matter experts, and derivative classifiers?
- _____ _____ _____ 72. Is refresher security training conducted at least annually and formally documented in writing to include the date of training, the subject covered, and list of attendees?
- _____ _____ _____ 73. Is there a continuing security awareness program that provides for frequent exposure of cleared personnel to security awareness information?
- _____ _____ _____ 74. Are termination briefings given to employees who leave the organization or whose clearance is terminated?

Industrial Security Program

- _____ _____ _____ 75. Does the CO issue and sign all DD 254s?
- _____ _____ _____ 76. Does the COR validate all contractor personal security clearances?
- _____ _____ _____ 77. Does the COR and NSI Representative verify FCL's and storage capability prior to release of classified information?
- _____ _____ _____ 78. Do the issued DD 254s provide additional security requirements?
- _____ _____ _____ 79. Does the COR verify that cleared contractor employees who are used as couriers have been briefed on their courier responsibilities?

Notes: _____

Submission of this form is to be received no later than September 30 of the current fiscal year by the NSI Program Team.
To expedite the process of submission, please fax the form to: 202-565-2028
ATTN: NSI Program Team

Date:	
NSI Representative Name:	
Program Office or Region:	
Program Name:	

Appendix E SAMPLES OF STANDARD FORMS

This page is intentionally blank



SF 706
Top Secret Label
(Orange)



SF 707
Secret Label
(Red)



SF 708
Confidential Label
(Blue)



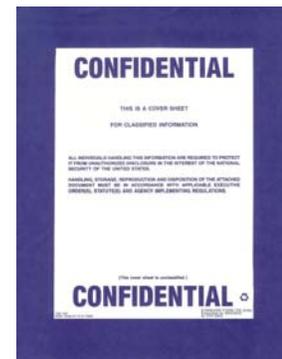
SF 710
Unclassified Label
(Green)



SF 703
Top Secret Cover Sheet
(Orange/White)



SF 704
Secret Cover Sheet
(Red/White)



SF 705
Confidential
Cover Sheet
(Blue/White)



SECURITY CONTAINER INFORMATION INSTRUCTIONS		CLASSIFICATION LEVEL		
1. Complete Part 1 and Part 2A (on end of flap). 2. Detach Part 1 and attach to the inside of the control drawer of the security container. 3. Mark Parts 2 and 2A with the highest classification level stored in the security container. 4. Detach Part 2A, insert in envelope (Part 2) and seal. 5. See Privacy Act Statement on reverse.		1. AREA OR POST <i>(if required)</i>	2. BUILDING <i>(if required)</i>	3. ROOM NO.
		4. ACTIVITY <i>(Division, Branch, Section or Office)</i>		5. CONTAINER NO.
		6. MFG. & CLASS OF CONTAINER	7. MFG. & LOCK MODEL	8. SERIAL NO. OF LOCK
9. DATE COMBINATION CHANGED	10. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE.			
11. <i>Immediately notify one of the following persons, if the container is found open and unattended.</i>				
EMPLOYEE NAME	HOME ADDRESS	HOME PHONE		

1. ATTACH TO INSIDE OF SECURITY CONTAINER 700-102 STANDARD FORM 700 (REV. 4-01)
 NSN 7540-01-214-5372 Prescribed by NARA/ISOO
 32 CFR 2003

WARNING
 WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS COPY MUST BE IN ACCORDANCE WITH
 APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CLASSIFICATION LEVEL _____

SECURITY CONTAINER NUMBER _____

COMBINATION

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A. INSERT IN ENVELOPE SF 700 (REV. 4-01)
 Prescribed by NARA/ISOO
 32 CFR 2003

Sample SF 700 (Security Container Information Form)

ACTIVITY SECURITY CHECKLIST		DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
Irregularities discovered will be promptly reported to the designated Security Office for corrective action.		Statement I have conducted a security inspection of this work area and checked all the items listed below.		
	TO (If required)	FROM (If required)	THROUGH (If required)	
ITEM				
1. Security containers have been locked and checked.	1	2	3	4
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.	5	6	7	8
3. Windows and doors have been locked (where appropriate).	9	10	11	12
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.	13	14	15	16
5. Security alarm(s) and equipment have been activated (where appropriate).	17	18	19	20
	21	22	23	24
	25	26	27	28
	29	30	31	
INITIAL FOR DAILY REPORT				
TIME				

701-101
NSN 7540-01-213-7899

USP LVN Printed on Recycled Paper

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOC
32 CFR 2003

Sample SF 701 (Activity Security Checklist)

Appendix F ROOM ACCREDITATION CHECKLIST

This page is intentionally blank

Room Accreditation Checklist

Accreditation Number _____

Section A Secure Area Information		
1. Type of Accreditation Request: (select one) <input type="checkbox"/> New Accreditation <input type="checkbox"/> Change / Upgrade	2. Level of Classified Information in the Room (mark all that apply) <input type="checkbox"/> Top Secret <input type="checkbox"/> Secret <input type="checkbox"/> Confidential	3. Room will be used for: (mark all that apply) <input type="checkbox"/> Classified Information Review <input type="checkbox"/> Classified Discussions <input type="checkbox"/> Classified Processing <input type="checkbox"/> Classified Storage <input type="checkbox"/> Classified Destruction <input type="checkbox"/> Secure Telephone <input type="checkbox"/> Secure Fax
4. Indicate Type of Area: (select one) <input type="checkbox"/> Continuous Handling (24 hr Open Storage) <input type="checkbox"/> Non-Continuous Handling (Closed Storage)	5. Justification for Accreditation: (continue on separate page if needed)	
6. Room Location Information: EPA Region: Program Name: Room Occupant: Bldg Name: Floor: Room Number: Street: City: State: Zip Code:		7. Responsible NSI Representative: NSI Representative: Work Phone: Fax Number: Secure Phone: Secure Fax Number:
8. Has the room been accredited before? <input type="checkbox"/> Yes (complete block 9) <input type="checkbox"/> No	9. Prior Accreditation Information: (if applicable) Accreditation Number: Accreditation Granted By: Accreditation Date:	

Room Accreditation Checklist

Accreditation Number _____

Section B	
Room Access Control Feature(s)	
<p>1. Is there a system in use that controls entry and visitor access to the room?</p> <p><input type="checkbox"/> Yes (complete block 2)</p> <p><input type="checkbox"/> No</p>	<p>2. Describe the type of entry and access control(s).</p> <p><input type="checkbox"/> Card Reader</p> <p><input type="checkbox"/> Passes or ID Badges</p> <p><input type="checkbox"/> Access List</p> <p><input type="checkbox"/> Visitor Escort</p> <p><input type="checkbox"/> Other:</p>
Section C	
Room Construction Features	
<p>1. Walls, Ceilings, and Floors</p> <p>a. Do the perimeter walls extend from true floor to true ceiling?</p> <p><input type="checkbox"/> Yes (complete block 2)</p> <p><input type="checkbox"/> No</p> <p>b. Are the perimeter walls permanently constructed?</p> <p><input type="checkbox"/> Yes (complete block 2)</p> <p><input type="checkbox"/> No</p> <p>c. Are the perimeter walls attached to each other? (i.e. NOT cubicles)</p> <p><input type="checkbox"/> Yes (complete block 2)</p> <p><input type="checkbox"/> No</p> <p>d. Is the ceiling a false ceiling? (open storage only)</p> <p><input type="checkbox"/> Yes (complete block 3)</p> <p><input type="checkbox"/> No</p> <p>e. Is the floor a false floor? (open storage only)</p> <p><input type="checkbox"/> Yes (complete block 4)</p> <p><input type="checkbox"/> No</p> <p>f. Do vent ducts penetrate the walls (open storage only)</p> <p><input type="checkbox"/> Yes (complete 5)</p> <p><input type="checkbox"/> No</p>	<p>2. Describe material and thickness of the room's perimeter walls, ceiling, and floors.</p> <hr/> <p>3. What is the distance between the false ceiling and the true ceiling?</p> <hr/> <p>4. What is the distance between the false floor and the true floor?</p> <hr/> <p>5. If vent ducts are over 6" in its smallest dimension or over 96 sq inches, describe the type of protection used. (e.g. 1/2" steel bars, expanded metal grills, commercial sound baffles, or intrusion detection system).</p>

Room Accreditation Checklist

Accreditation Number _____

Room Construction Features (continued)

<p>6. Doors</p> <p>a. Type of door(s). (complete block 7)</p> <p><input type="checkbox"/> Wood</p> <p><input type="checkbox"/> Metal</p> <p>b. Do/does the door(s) have a solid core?</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>c. Location of door hinges.</p> <p><input type="checkbox"/> Interior to the space</p> <p><input type="checkbox"/> Exterior to the space (complete block 8 if in an uncontrolled area)</p> <p>d. Type of lock on door.</p> <p><input type="checkbox"/> Electronic (X07, X08, X09) (complete block 9)</p> <p><input type="checkbox"/> Cypher (complete block 9)</p> <p><input type="checkbox"/> Keyed</p> <p><input type="checkbox"/> None</p>	<p>7. Describe the room entrance and exit door(s). (e.g. number, thickness, windows, automatic door closer, deadbolts, panic hardware)</p>
	<p>8. Describe how the door hinges exterior to the room are secured against removal. (e.g. welded)</p>
	<p>9. Where is the door lock combination stored?</p>
<p>10. Windows</p> <p>a. Does the space have windows?</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No (proceed to section D)</p> <p>b. How are windows protected against visual surveillance?</p> <p><input type="checkbox"/> Opaque glass</p> <p><input type="checkbox"/> Drapes/Curtains</p> <p><input type="checkbox"/> Blinds</p> <p><input type="checkbox"/> Other (complete block 11)</p> <p>c. Are windows at the ground level?</p> <p><input type="checkbox"/> Yes (complete block 12)</p> <p><input type="checkbox"/> No</p> <p>d. Are ground windows monitored with an IDS?</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> Not Applicable</p>	<p>11. Describe window covering.</p>
	<p>12. If windows are at ground level, describe how they are secured against opening. (e.g. permanent seal, locking mechanism)</p>

Room Accreditation Checklist

Accreditation Number _____

Section D Room Sound Attenuation	
<p>1. With all doors closed, check which best describes the sound barrier performance of walls, ceilings, floors, windows, and doors.</p> <p><input type="checkbox"/> Normal speech can be heard and understood</p> <p><input type="checkbox"/> Normal speech can be heard but not understood</p> <p><input type="checkbox"/> Loud speech can be understood fairly well. Normal speech cannot be easily understood.</p> <p><input type="checkbox"/> Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly if at all.</p> <p><input type="checkbox"/> Loud speech can be faintly heard but not understood. Normal speech is unintelligible.</p> <p><input type="checkbox"/> Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume, can be heard only faintly or not at all.</p>	<p>2. Does the space utilize sound cover or masking? (Complete Block 3)</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <hr/> <p>3. Describe the type of sound cover or masking utilized. (e.g. white/pink noise, wall mounted transducer, cd player, television, etc.)</p>
Section E Classified Equipment in Room	
<p>1. Describe the type of secure phone issued. (if applicable)</p> <p><input type="checkbox"/> STE <input type="checkbox"/> STU-III</p> <p>Classification level of encryption key:</p> <p><input type="checkbox"/> Secret <input type="checkbox"/> Top Secret</p> <p>Make/Model: Secure Phone #:</p>	<p>4. Is there a classified computer used in the room?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>5. Classification level of computer:</p> <p><input type="checkbox"/> Confidential <input type="checkbox"/> Secret <input type="checkbox"/> Top Secret</p>
<p>2. Describe the type of secure facsimile: (if applicable)</p> <p>Make: Model:</p>	<p>6. Describe the type of classified computer used in the room: (e.g. laptop, desktop)</p>
<p>3. Describe the type of NSA approved shredder: (if applicable)</p> <p>Make: Model:</p>	<p>7. SSAA registration number:</p>
Section F Storage Container in Room	
<p>1. Will classified be stored in this space?</p> <p><input type="checkbox"/> Yes (complete block 3)</p> <p><input type="checkbox"/> No</p> <p>2. Level of classified storage required?</p> <p><input type="checkbox"/> Top Secret <input type="checkbox"/> Secret <input type="checkbox"/> Confidential</p>	<p>3. Type of container utilized?</p> <p><input type="checkbox"/> GSA approved class 5 or 6 safe</p> <p style="padding-left: 20px;"><input type="checkbox"/> Legal size <input type="checkbox"/> Letter size <input type="checkbox"/> Other:</p> <p>Container Make and Serial Number(s):</p>

Room Accreditation Checklist

Accreditation Number _____

Section G Supplemental Controls		
<p>1. Choose one of the supplemental controls that is being utilized: (open storage area and secure area with TS storage only)</p> <p><input type="checkbox"/> The location that houses the open storage area is under continuous (24 hr) protection by cleared guard or duty personnel; (complete block 2)</p> <p><input type="checkbox"/> Inspection of the open storage area is conducted by cleared guards or security personnel every 2 hours for Top Secret information and 4 hrs for Secret and Confidential information); (complete block 2)</p> <p><input type="checkbox"/> An Intrusion Detection System (IDS) is installed with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation for Top Secret information and within 30 minutes for Secret and Confidential information; (complete block 3 and 4)</p> <p><input type="checkbox"/> Security-In-Depth conditions provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740</p>	<p>2. Clearance level of guards:</p> <p><input type="checkbox"/> None <input type="checkbox"/> Top Secret</p> <p style="padding-left: 100px;"><input type="checkbox"/> Secret</p> <p style="padding-left: 100px;"><input type="checkbox"/> Confidential</p>	
<p>3. Define the type of IDS utilized.</p> <p><input type="checkbox"/> Motion Detection</p> <p><input type="checkbox"/> Alarms</p> <p><input type="checkbox"/> Other: _____</p> <p>Note: Provide IDS specification with submission of this form.</p>		<p>4. Where is the IDS monitored?</p>
Section H Additional Required Information		
<p>1. Provide one of the following:</p> <p><input type="checkbox"/> Floor plan sketch of the area for accreditation (showing dimensions) and the immediate surrounding area/offices.</p> <p><input type="checkbox"/> Design Intent Drawings (if building out the area from scratch)</p>		
Section I Signature Block		
<p>1. Requester Name:</p>	<p>2. Date:</p>	<p>3. Requester Signature:</p>
<p>4. NSI Representative or NSI Program Team Member Name:</p>	<p>5. Date:</p>	<p>6. Signature: I have verified that all the information above is correct.</p>

This page is intentionally blank

Appendix G ACCREDITATION STATUS FORM

This page is intentionally blank

Secure Room Accreditation Status Form

Secure Area Information			
Type of Accredited Room: <input type="checkbox"/> Open Storage Area <input type="checkbox"/> Secure Area	Level of Accreditation: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C	Region, Facility Name, Address:	Responsible NSI Representative: Name: Phone: Email:
Accreditation Number:		Accreditation Official:	Accreditation Date:
Section A - Accreditation Status/Request			
To be completed by the NSI Representative			
<input type="checkbox"/> Accreditation Suspended <input type="checkbox"/> Request Recertification <input type="checkbox"/> Request Withdrawal		Action or Reason: <div style="font-size: x-small; margin-top: 10px;">My signature confirms that I have verified the continued accuracy of the Secure Room Accreditation Checklist.</div>	
NSI Representative:		Date:	Signature:
Section B - Accreditation Recertification			
To be completed by the NSI Program Team			
<input type="checkbox"/> Action Required <input type="checkbox"/> Approved <input type="checkbox"/> Disapproved		Action or Reason:	
Accreditation Official Name:		Date:	Signature:
Section C - Accreditation Withdrawal			
To be completed by the NSI Program Team			
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved		Reason:	
Accreditation Official Name:		Date:	Signature:

This page is intentionally blank

Appendix H CLASSIFIED INFO ACCOUNT RECORD

This page is intentionally blank



United States Environmental Protection Agency
Washington, DC 20460

EPA Control Number

Classified Information Accountability Record

Section I. General

To:	From:
-----	-------

Date Transferred	Registered Mail Number
------------------	------------------------

Section II. Description

Serial Number	Date of Information	Item Description (unclassified whenever possible)	Copy Number	Classification

Section III. Receipt / Tracer Action (Check appropriate block)

<input type="checkbox"/> Receipt of information acknowledged	<input type="checkbox"/> Tracer: Signed receipt has not been received
--	---

Date	Printed Name	Signature
------	--------------	-----------

Section IV. Internal Routing

To	Copy No.	Date	Typed or Printed Name	Signature of Recipient
1.				
2.				

Section V. Reproduction Authority (If restricted by the Originating Agency)

No. of Copies To Be Reproduced	Authorized by:	Date
--------------------------------	----------------	------

Section VI. Destruction Certificate (Top Secret only)

Information Described Hereon Has Been Destroyed

Office Symbol	Date	Printed Name of NSI Representative	Signature
Destruction Record Number	Date	Printed Name of Destruction Official	Signature
Page or Copy Number	Date	Printed Name of Witnessing Official	Signature

This page is intentionally blank

Appendix I COURIER DOCUMENTATION

This page is intentionally blank



1. I understand that I am authorized to courier classified material and that my courier card authorizes me to hand carry classified information. I further understand that if I have a requirement to hand carry via commercial transportation or require an overnight stay, I will obtain authorization from the NSI Representative.
2. I understand the classified material must be in my physical possession at all times, and I may not read, study, display, or use classified material in any manner on a public conveyance, in a public place, or at my home. Upon arrival, I will transfer the classified material to the authorized government or contracting facility representative accepting responsibility for safeguarding the package.
3. I will ensure classified material is double wrapped and appropriately marked. An envelope may serve as the inner wrapper and a locked zipper pouch or locked briefcase may serve as the outer cover.
4. When classified material is transported in an automobile, I will not place it in any detachable storage compartment (e.g., automobile trailers, luggage racks), or in the trunk. It will be kept next to me at all times.
5. Prior to hand carrying classified material, I will provide a list of all classified material carried by me to my NSI Representative. Upon my return, the NSI Representative will account for all classified material, if necessary.
6. If an overnight stop is approved by the NSI Representative, he/she will assist with the advance arrangements for proper overnight storage in a Government or contractor facility. I will obtain a signed receipt from an authorized government or contracting facility representative accepting responsibility for safeguarding the package.
7. If travel is authorized, I understand that the material will be subject to routine security screening. Screening officials may check the sealed package, zippered pouch or closed briefcase by X-ray machine. Screening officials are not permitted to open the classified material. If security requests that I open the package, I will show my written authorization letter and inform security that the package contains U. S. Government classified information, and state that it cannot be opened. If there are further problems with security checkpoints, I will contact the Security Manager. If the issues are still not resolved, I will contact my NSI Representative or the OARM's NSI Program Team.
8. I will keep the classified material in my possession and in my sight and will not place the classified material in any storage or overhead compartment.
9. In the event of any emergency, delay, change in destination, and loss or compromise of classified material, I will immediately notify my NSI Representative or the NSI Program Team.
10. I understand that if my clearance status changes for any reason I must notify my NSI Representative or the NSI Program Team to inquire about any changes to my courier status or responsibilities.
11. I certify that I have read and understand the requirements to hand carry classified information. I will follow the procedures at all times when carrying classified materials.

Typed or Printed Name

Signature

Date Signed

Region / Program Office

Work Telephone Number

Courier Card #

This page is intentionally blank

OUT OF AREA COURIER PREPARATION CHECKLIST

SECTION I

To be completed by designated courier

1. Name(s): _____
2. Mode of Transportation: _____
3. Destination: _____
4. Itinerary: (attach the airline itinerary or map showing driving route)
5. Security Representative (Origin):

Name	() - Work Phone Number	() - Alternate Contact Number
------	----------------------------	-----------------------------------
6. Security Representative (Destination):

Name	() - Work Phone Number	() - Alternate Contact Number
------	----------------------------	-----------------------------------
7. Alternate Contact (Destination):

Name	() - Work Phone Number	() - Alternate Contact Number
------	----------------------------	-----------------------------------
8. Emergency Contact:

Name	() - Work Phone Number	() - Alternate Contact Number
------	----------------------------	-----------------------------------

SECTION II

To be completed by a security representative

	YES	N/A
1. Presented a valid Courier Card(s)	<input type="checkbox"/>	---
2. Packaged and Sealed Material	<input type="checkbox"/>	---
3. Completed the Classified Information Accountability Record	<input type="checkbox"/>	---
4. Received a signed "Authorization to Transport Classified Government Information aboard a Commercial Aircraft" Memorandum, when required	<input type="checkbox"/>	<input type="checkbox"/>
5. Obtained Maps, if driving	<input type="checkbox"/>	<input type="checkbox"/>
6. *Debriefed After Trip	<input type="checkbox"/>	---

* The debriefing must be given upon the return of ALL "Out of Local Area" trips by the NSI Representative. The debriefing is intended to identify if the courier encountered any problems and document any abnormal occurrences. The NSI Representative shall provide the NSI Program Team with documentation of all problems, occurrences, or procedural weaknesses. This checklist is to be maintained for the duration of the trip it documents; however, if there are any incidents identified during the debriefing, all material must be retained as part of the incident record.

Completing the “Out of Area Courier Preparation Checklist”

SECTION I This section is to be completed by the courier.

1. **Name(s):** List the courier(s) responsible for transporting the classified material.
2. **Mode of Transportation:** Identify the type of transportation being used (i.e., commercial aircraft, train, automobile).
3. **Itinerary:** Attach the itinerary. This should include: departure and arrival dates, times, and location. If aircraft or train, it should include specific information including: carrier and aircraft/train identification number and connections/layovers/transfers. If driving, attach a map identifying driving route and estimate the trip travel time. If trip includes returning with classified information, include the return itinerary.
4. **Security Representative (Origin):** If departing from EPA, list the Program or Regional NSI Representative and work/alternate contact numbers. If departing from another agency, identify the security representative, and work/alternate contact numbers. Ensure the security representative identified is aware of travel plans and material carried. Phone numbers are required for emergency purposes.
5. **Security Representative (Destination):** Identify the security representative and work/alternate contact numbers. This individual should be aware of the travel plans and anticipated arrival time. The security representative should be notified upon arrival, and he/she can help properly store the material. Additionally, he/she can be contacted in case of emergency.
6. **Alternate Contact (Destination):** Designate an alternate contact at the destination. This individual does not need to be a security representative; however he/she is required to have a security clearance and access to a security container that is authorized for storage of classified information. As the alternate contact, he/she should be aware of the travel plans and anticipated arrival time.
7. **Emergency Contact Phone Number:** Designate an emergency contact. Ideally, this individual is a security professional and is available if no other designated personnel can be contacted. This individual should be aware of travel itinerary and anticipated arrival time.

SECTION II This section is to be completed by a security representative. To authorize the out of area courier travel, the security representative shall check each of the following items:

1. Does the courier have a valid courier card? The NSI Handbook, Chapter 6, Section 500 identifies the requirements for hand-carrying classified information out of EPA controlled space. Courier cards are issued to EPA federal and non-federal employees to indicate an individual has been designated to officially carry classified information on behalf of the U.S. Government.
2. Has material been properly wrapped and packaged for transportation? The NSI Handbook, Chapter 6, Section 300 identifies the requirements for correctly double wrapping classified information.
3. Has the courier completed the Classified Information Accountability Record? Records to document the transmission of classified information must be created and maintained in accordance with the NSI Handbook, Chapter 6, Section 200.
4. Has the security representative issued an “Authorization to Transport Classified Government Information aboard a Commercial Aircraft” Memorandum? This memorandum, identified in the NSI Handbook, Chapter 6, Section 503, is designed to indicate that the courier has been designated to officially carry classified information on behalf of the U.S. Government. The intention is to mitigate the any problems, which the courier might encounter. While providing justification for not permitting the package to be opened, seized, or inspected.
5. Has the courier obtained maps, if driving? Maps are required as part of the submitted itinerary. The map should indicate the courier’s driving route to his/her destination. The map is required to be part of the itinerary in case of emergencies. Additionally, submitting a driving route will assist a courier with time estimation. An additional map should be maintained and used by the courier en route.
6. Was a debriefing provided following the trip? Debriefings are intended to identify if the courier encountered any problems and document any abnormal occurrences. The NSI Representative shall provide the NSI Program Team with documentation of all problems, occurrences, or procedural weaknesses. This checklist and all supplemental documentation are to be maintained for the duration of the trip which it documents.

(date)

MEMORANDUM

SUBJECT: Authorization to Transport Classified Government Information aboard a Commercial Aircraft

FROM: (NSI Representative Name and EPA Program Office or Region)

TO: Whom it May Concern

This letter is to certify that the individual below has been identified as an official courier of U.S. Government classified National Security Information:

Name:

The individual has in his/her possession the following picture identification, which may be reviewed to confirm identification:

Photo Identification Type:

Photo Identification Number:

Expiration Date of Identification:

The following is a description of package being carried:

(Provide unclassified description of physical appearance of package)

Under no circumstances are the containers/packages under his/her control to be inspected, opened or seized. All Federal, State, and Local authorities, Special Police, and other law enforcement officers are requested to render assistance in the event of an emergency. Verification of courier authorization, additional information and/or assistance can be obtained by calling the undersigned at the phone number provided.

(Name)

(Phone)

This page is intentionally blank

Appendix J FGI CLASSIFICATION MATRIX

This page is intentionally blank

FGI Classification Matrix

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
ARGENTINA	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
AUSTRALIA	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
AUSTRIA	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
BELGIUM	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERTKE VERSPREIDING
BOLIVIA	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
BRAZIL	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
CAMBODIA	SAM NGAT BAMPHOT	SAM NGAT	ROEUNG ART KAMBANG	HAM KOM PSAY
CANADA	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
CHILE	SECRETO	SECRETO	RESERVADO	RESERVADO
COLUMBIA	ULTRA SECRETO	SECRETO	RESERVADO	CONFIDENCIALRESTRINGIDO
COSTA RICA	ALTO SECRETO	SECRETO	CONFIDENCIA	
DENMARK	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
ECUADOR	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO
EL SALVADOR	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
ETHIOPIA	YEMIAZ	BIRTOU MISTIR	MISTIR KILKIL	
FINLAND	ERITAIN SALAINEN	SALAINEN		
FRANCE	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
GERMANY	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	
GREECE	AKPOE AΠOΠHTON	AΠOΠHTON	EMΠΙΣΤΕΥΤΙΚON	ΠΙΠΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ
GUATAMALA	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
HAITI	TOP SECRET	SECRET	CONFIDENTIAL	RESERVE
HONDURAS	SUPER SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
HONG KONG	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
HUNGARY	SZIGORUAN TITKOS	TITKOS	BIZALMAS	
INDIA	PARAM GUPT	GUPT	GOPNIYA	PRATIBANHST/SEEMIT
INDONESIA	SANGAT RAHASIA	RAHASIA AGAK	RAHAHASIA	TERBATAS
IRAN	BEKOLI SERRI	SERRI	KHEIL MAHRAMANEH	MAHRAMANEH
IRAQ	SIRRI LIL-GHAXEH	SIRRI	KHASS	MEHDOUD
ICELAND	ALGJORTI	TRUNADARMAL		
IRELAND	AN-SICREIDEACH	SICREIDEACH	RUNDA	SRIANTA
ISRAEL	SODI BEYOTER	SODI	SHAMUR	MUGBAL
ITALY	SEGRETISIMO	SECRETO	RISERVATISSIMO	RISERVATO
JAPAN	KIMITSU	GOKUHI	HI	TORIATSUKAICHUI
JORDAN	MAKTUM JIDDAN	MAKTUM	SIRRI	MAHDUD
KOREA	I-KUP BI MIL	II-KUP BI MIL	III-KUP BI MIL	BU WOI BI
LAOS	LUP SOOD GNOD	KUAM LUP	KUAM LAP	CHUM KUT KON ARN
LEBANON	TRES SECRET	SECRET	CONFIDENTIEL	
MALAYSIA	RAHSIA BESAR	RAHSIA	SULIT	TERHAD
MEXICO	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
NETHERLANDS	ZEER GEHEIM	GEHEIM	CONFIDENTIEEL or DIENSTGEHEIM	VERTROUWELIJK
NEW ZEALAND	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
NICARAGUA	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
NORWAY	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELL	BEGRENSET
PAKISTAN	INTAKAI KHUFIA	KHUFIA	SIGHA-E-RAZ	BARAI MAHDUD TAQSIM
PARAGUAY	SECRETO	SECRETO	CONFIDENCIAL	RESERVADO

Security Features Description

PERU	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
PHILIPPINES	TOP SECRET	SECRET	CONFIDENCIAL	RESTRICTED
PORTUGAL	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
SAUDI ARABIA	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET	SAUDI RESTRICTED
SPAIN	MAXIMO SECRETO	SECRETO	CONFIDENCIAL	DIFFUSION LIMITADA
SINGAPORE	TOP SECRET	SECRET	CONFIDENCIAL	RESTRICTED
SWEDEN (Red Borders)	HEMLIG	HEMLIG		
SWITZERLAND	(Three languages: French, German and Italian. TOP SECRET has a registration number to distinguish it from SECRET and CONFIDENTIAL)			
TAIWAN	CHICHIMI	CHIMI		
THAILAND	LUP TISUD	LUP MAAG	LUP	POK PID
TURKEY	COK GIZLI	GIZLI OZEL	HIZMETE	OZEL
UNION OF SOUTH AFRICA				
(English)	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
(Afrikaans)	UITERS GEHEIM	GEHEIM	VERTROULIK	BEPERK
UNITED ARAB REPUBLIC				
EGYPT	JIRRI LIL GHAXEH	SIRRI	KHAS	MEHOUD JIDDEN
UNITED KINGDOM	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
URUGUAY	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
USSR				
VIETNAM	TOI-MAT	MAT	KIN	PHO BIEN HAN CHE

Appendix K SECURITY FEATURE DESCRIPTIONS

This page is intentionally blank

Security Features Description

This Appendix provides detailed description of each technical security feature and associated assurance provided in Table 10-3 (Confidentiality), Table 10-4 (Integrity), and Table 10-5 (Availability).

Access Control

The classified information system shall store and preserve the confidentiality of all sensitive information internal to the system.

[Access 1] Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

[Access 2] Discretionary access controls shall be utilized in the system. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

[Access 3] The systems shall employ a process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals (e.g., compartments into which users are briefed) granted to another user. The system shall also employ a process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

Account Management Procedures

[AcctMan] Account management procedures that include identifying types of accounts (individual and group, conditions for group membership, associated privileges), establishing an account (i.e., required paperwork and processes), activating an account, modifying an account (i.e., disabling an account, changing privilege level, group memberships, authenticators), and terminating an account (i.e., processes and assurances).

Audit Capability

Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

[Audit 1] Audit analysis and reporting shall be scheduled and performed. Security relevant events shall be documented and reported. The contents of audit trails shall be protected against unauthorized access, modification, or deletion. The frequency of the review shall be documented in the SSAA. Audit records shall be retained for at least one review cycle. Audit records shall be created to record the following:

- Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved

Security Features Description

- Successful and unsuccessful logons and logoffs
- Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion
- Changes in user authenticators
- The blocking or blacklisting of a UserID, terminal, or access port and the reason for the action
- Denial of access resulting from an excessive number of unsuccessful logon attempts

[Audit 2] In addition to Audit 1, individual accountability shall be enforced (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). The ISSR is required to periodically test the security posture of the system by employing various intrusion or attack detection and monitoring tools.

[Audit 3] In addition to Audit 1 and 2, audit analysis and reporting shall be scheduled and performed using automated tools.

[Audit 4] In addition to Audit 1, 2, and 3, an audit trail shall be created and maintained by the system that is capable of recording changes to the mechanism's list of user formal access permissions. (Note: Applicable only if the [Access 3] access control mechanism is automated.)

Backup Power

An alternate power source (e.g., battery or generator) ensures that system availability is maintained in the event of a loss of primary power. An alternate power source can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

[Power 1] Procedures for the graceful shutdown of the system shall ensure no loss of data. Battery backup power is adequate to allow the system to be fail-safe. The decision not to use an alternate source of power (e.g., battery, UPS) for the system shall be documented in the SSAA.

[Power 2] Procedures shall be developed for the transfer of the system to an alternate power source. These procedures shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

Backup Procedures

The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic review of backup inventory and its restorability of information validates that the process is working. The frequency of backups shall be defined in the SSAA.

[Backup 1] Procedures for the regular backup of all essential and security-relevant information, including software, router tables, settings, and documentation, shall be recorded.

Security Features Description

[Backup 2] In addition to Backup 1, media containing backup files and backup documentation shall be stored at another location (i.e., part of the same building, a nearby building, or off-site facility). This will reduce the possibility that a common occurrence could eliminate both on-site and off-site facility backup data. Backup procedures shall also be periodically verified.

[Backup 3] In addition to Backup 1 and 2, incremental and complete restoration of information from backup media shall be tested on an annual basis.

Change Control

The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to ensuring that only authorized changes are allowed.

[Change 1] Procedures and technical system features shall be implemented to ensure that changes to the data and software are executed only by authorized personnel or processes.

[Change 2] In addition to Change 1, a secure, unchangeable audit trail will be implemented to facilitate the correction of improper data changes.

Data Transmission

Cryptography is a critical tool used to protect confidentiality of data, to assure the authenticity of information, and to detect the alteration of information. National policy requires National Security Agency (NSA) to review and approve all cryptography used to protect classified information from access by unauthorized persons. The following protection shall be used for all electronic transmissions outside the defined system parameter:

[DataTrans] National Security Agency (NSA) - approved encryption mechanisms appropriate for the encryption of classified information.

Identification and Authentication

[I&A 1] Procedures shall be included that provide for uniquely identifying and authenticating the users. Procedures can be external to the system (e.g., procedural or physical controls) or internal to the system (i.e., technical). Electronic means shall be employed where technically feasible.

[I&A 2] Procedures shall be included that provide for an I&A management mechanism that ensures a unique identifier for each user which associates that identifier with all auditable actions taken by the user. The following must be specified in the SSAA:

- Initial authenticator content and administrative procedures for initial authenticator distribution
- Individual and Group Authenticators - Group authenticators may only be used in conjunction with an individual/unique authenticator (i.e., individuals must be authenticated with an individual authenticator prior to use of a group authenticator)

Security Features Description

- Length, composition, and generation of authenticators
- Change processes (periodic and possible compromise)
- Aging of static authenticators (i.e., not one-time passwords or biometric patterns)
- History of authenticator changes, with assurance of non-replication
- Protection of authenticators

[I&A 3] In addition to I&A 2, access to the classified information system by privileged users who either reside outside of the designated system's perimeter or whose communications traverse data links that are outside the system's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

[I&A 4] In those instances where the means of authentication are user-specified passwords, the ISSO may employ (with the approval of the ISSM) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password.

[I&A 5] In those instances where the users are remotely accessing the classified information system, the users shall employ a strong authentication mechanism.

Least Privilege

[LeastPrv] Assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks shall be employed.

Malicious Code

[MalCode] Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-virus software).

Resource Control

[ResrcCtrl] The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

Security Documentation (Doc)

[Doc 1] Documentation shall include a System Security Authorization Agreement (SSAA). The System Owner is responsible for preparing the security agreement, implementing the plan, and monitoring its effectiveness. The format for the SSAA is provided in the National Information Assurance Certification and Accreditation Process (NIACAP) described in the National Security and Telecommunications Information System Security Instruction No. 1000 (NSTISSI No. 1000). SSAAs are living documents that require periodic reviews, modification, and milestones or completion dates for planned controls. The CONOPS shall, at a minimum, include a description of the

Security Features Description

system's purpose, architecture, accreditation schedule, Protection Level, and Level-of-Concern for integrity, availability, and confidentiality.

[Doc 2] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall, at a minimum, provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.

[Doc 3] The DAA may also direct documentation to include certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level, reports of test results, and a general user's guide which describes the protection mechanisms and provides guidelines on how the mechanisms are to be used.

Security Testing

Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSO/ISSR will perform and document the required tests.

[Test 1] Assurance shall be provided to the ISSM that the system operates in accordance with the approved SSAA and that the security features, including access controls, are implemented and operational.

[Test 2] Written assurance shall be provided to the ISSM that the classified system operates in accordance with the approved SSAA, and that security features, including access controls and discretionary access controls, are implemented and operational.

[Test 3] Certification testing shall be conducted to include a verification that features and assurances required for the Protection Level are functional. A test plan and procedures shall be developed to include:

- A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability
- A detailed description of the assurances that have been implemented, and how this implementation will be verified
- An outline of the inspection and test procedures used to verify this compliance

Separation of Function

[Separation] The functions of the ISSO/ISSR and the System Administrator shall not be performed by the same person.

Security Features Description

Session Controls

Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user's session.

[SessCtrl 1] The following shall be applied:

- User Notification - All users shall be notified, prior to gaining access to a system, that system usage is monitored, recorded, and subject to audit
 - The user shall also be advised that, by using the system, the individual has granted consent to such monitoring and recording
 - The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties
 - If the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user, and the user shall be required to take positive action to remove the notice from the screen
 - The ISSM will provide an approved banner
 - Electronic means shall be employed where technically feasible
 - If it is not possible to provide an "initial screen" warning notice, other methods of notification shall be developed and approved by the ISSM
- Successive Logon Attempts - If the operating system provides the capability, successive logon attempts shall be controlled as follows:
 - By denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same UserID
 - By limiting the number of access attempts in a specified time period
 - By the use of a time delay control system
 - By other such methods, subject to approval by the ISSM
- System Entry - System entry shall be granted only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.
- Screen Lock – Screen lock functionality shall be associated with each computer monitor, unless there is an overriding technical or operational problem. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen, totally hiding what was previously visible. Screen lock capability shall:
 - Be enabled either by explicit user action or if the system is left idle for a specified period of time (e.g., 15 minutes or more)
 - Ensure that once the system security/screen-lock software is activated, access to the system requires knowledge of a unique authenticator
 - Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded)

Security Features Description

[SessCtrl 2] In addition to SessCtrl 1, the following shall be applied:

- Multiple Logon Control - If the classified information system supports multiple logon sessions for each UserID or account, the classified system shall provide a protected capability to control the number of logon sessions for each UserID, account, or specific port of entry
 - The classified system default shall be a single logon session
- User Inactivity - The classified system shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator
 - The inactivity time period and restart requirements shall be documented in the SSAA
- Logon Notification - If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon, the location of the user (as can best be determined) at last logon, and the number of unsuccessful logon attempts using this UserID
 - This notice shall require positive action by the user to remove the notice from the screen

System Assurance

System assurance includes those components of a system (hardware, software, firmware, and communications) essential to maintaining the security policy(ies) of the system.

[SysAssur 1] Access to hardware/software/firmware that perform system or security functions shall be limited to authorized personnel.

[SysAssur 2] In addition to SysAssur 1, the protections and provisions of the system assurance shall be documented. Features and procedures shall exist to periodically validate the correct operation of the hardware, software, and firmware elements of the security policy(ies), and shall be documented in the SSAA.

System Recovery (SR)

System recovery addresses the functions that respond to failures in the system security protection features or interruptions in operation. Recovery actions ensure that the system security protection is returned to a condition where all security-relevant functions are operational, or system operation is suspended.

[SR 1] Classified information system features and procedures shall be implemented to ensure that systems recovery is done in a controlled manner. If any unusual conditions arise during recovery, the system shall be accessible only via terminals monitored by the ISSO/ISSR, or via the classified information system console.

This page is intentionally blank

Appendix L SCI AUTHORIZATION REQUEST FORM

This page is intentionally blank



United States Environmental Protection Agency
Washington, DC 20460

SCI Authorization Request Form

Date:

Section 1: Requester Information and Justification This section is to be completed by the Requester, and validated, by signature, from the Program or Regional Office Director.

Name:

Program Office:

Division:

Job Title:

Access(es) Required: Identify the SCI access(es) required to complete job requirements.

Justification: Attach a comprehensive unclassified rationale why SCI access is required.

I acknowledge that the justification provided is accurate, and the Requester requires for SCI access.

Print Name:

Signature:

Date:

Section 2: Clearance Data This section is to be completed by the NSI Program Team SSO

I validate that the Requester meets the investigation and clearance requirements. The information is as follows:

Clearance Level: _____

Investigation Type: _____

Date Granted: _____

Date Completed: _____

Print Name:

Signature:

Date:

Section 3: Authorization for SCI Adjudication This section is to be completed by the Office of the Administrator

I have reviewed the justification provided, and _____ that this employee should be submitted for SCI access.

Agree

Disagree

Print Name:

Signature:

Date:

NOTE: The NSI Program Team requires original signature for each section of this document. To expedite processing, fax the form to the NSI Program Team at: 202-565-2028; however, the form shall also be forwarded to the NSI Program Team at:

U.S. EPA
Security Management Division
ATTN: NSI Program Team
1300 Pennsylvania Ave, NW
Mail Code: 3206R, Room G.1-1
Washington, D.C. 20004

This page is intentionally blank

Appendix M SCI VISIT CERTIFICATION REQUEST FORM

This page is intentionally blank



United States Environmental Protection Agency
Washington, DC 20460

Date:

SCI Visit Certification Request Form

Email the completed form, at least five days prior to your visit, to the NSI Program Team at: ProgramTeam.nsi@epa.gov Include the form's name in the e-mail subject line.

Name:

Recurring Event:

- Yes
 No

Dates Required:

_____ to _____

Access(es) Required:

Place of Visit:

Address:

Purpose for Visit:

Point of Contact:

Phone Number:

Security Officer:

Phone Number:

Fax Number:

This page is intentionally blank



December 2006

**Office of Administration and Resources Management,
National Security Information Program Team**

Phone: (202) 564-1983 Fax: (202) 565-2028

Email: ProgramTeam.nsi@epa.gov

Intranet Web: <http://intranet.epa.gov/oas/smd/nationalsec.htm>