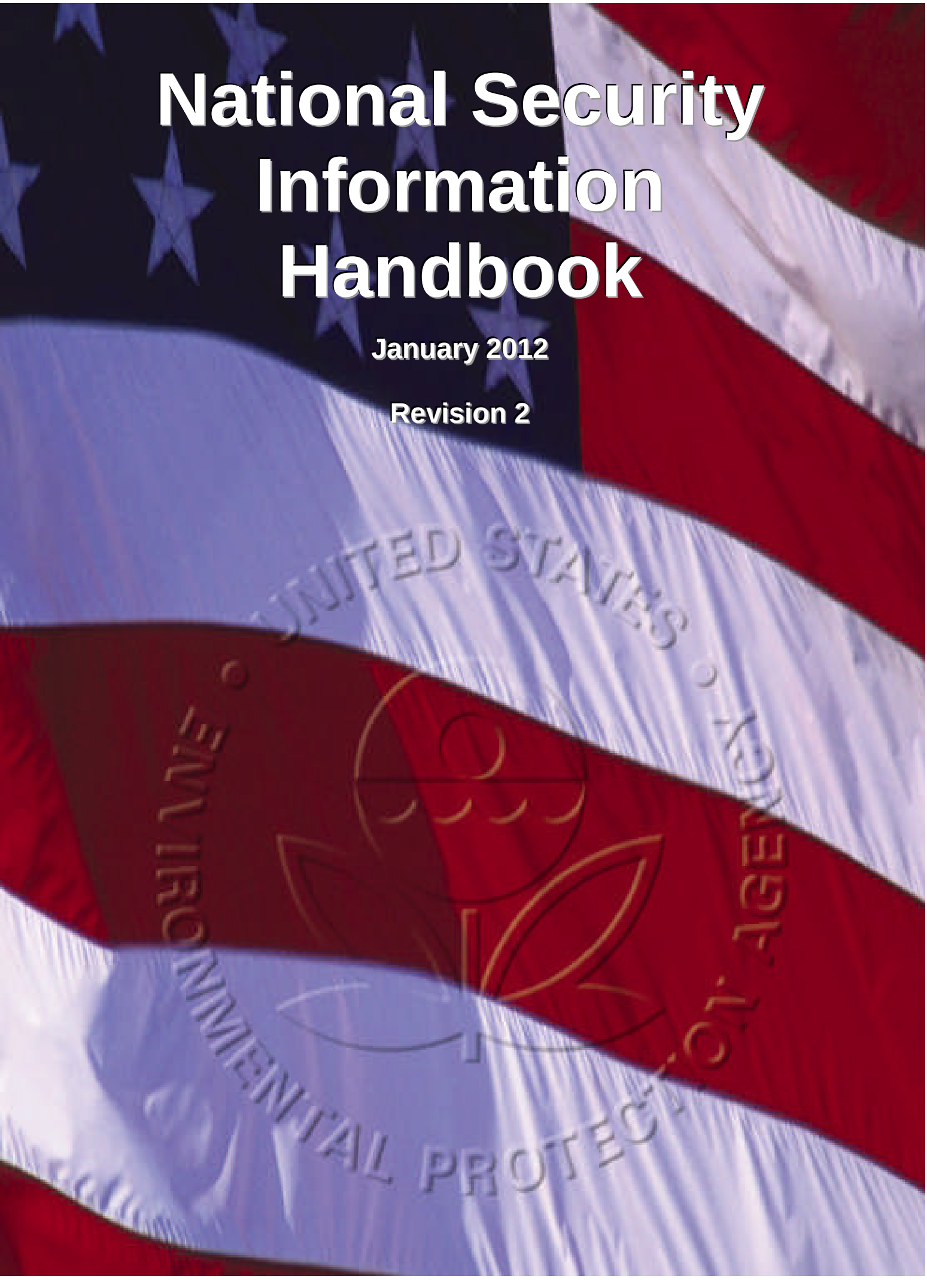
National Security Information Handbook

January 2012

Revision 2



This page is intentionally blank

TABLE OF CONTENTS

This page is intentionally blank

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AA Assistant Administrator
AO Administrator's Office, EPA
C Confidential
CCI Controlled Cryptographic Item
CD Compact Disk
CFR Code of Federal Register
CIA Central Intelligence Agency
CNSS Committee on National Security Systems
CO Contracting Officer
COMSEC Communications Security
CMCS COMSEC Material Control System
CONOPS Concept of Operations
COR Contracting Officers Representative
CSIRT Computer Security Incident Response Team
CTS Customer Technology Solutions
CVS Clearance Verification System
DAA Designated Approving Authority
DCID Director of Central Intelligence Directive
DCS Defense Courier Service
DD Department of Defense (Forms Only)
DIA Defense Intelligence Agency
DISCO Defense Industrial Security Clearance Office
DNI Director of national Intelligence
DoD Department of Defense
DSS Defense Security Services
E.O. Executive Order
EPA Environmental Protection Agency
EPL Evaluated Products List
FAR Federal Acquisition Regulation
FCL Facility Clearance (or Facility Security 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
HSDN Homeland Secure Data Network
HQ Headquarters
HVAC Heating, Ventilation, and Air Conditioning
IC Intelligence Community
ICD Intelligence Community Directive
ICPG Intelligence Community Policy Guidance
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 Systems Security Officer
ISSR	Information Systems Security Representative
IT	Information Technology
JAFAN	Joint Air Force, Army, Navy
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Communications System
LES	Law Enforcement Sensitive
MOA	Memorandum of Agreement
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NF	Not Releasable to Foreign Nationals, see also NOFORN
NFIP	National Foreign Intelligence Program
NIAP	National Information Assurance Partnership
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
NSSP	National Security Systems Program
NTISSAM	National Telecommunications and Information Systems Security Advisory/Information Memorandum
NTISSI	National Telecommunications and Information Systems Security Instruction
NOFORN	Not Releasable to Foreign Nationals, see also NF
OADR	Originating Agency's Determination Required
OARM	Office of Administration and Resources Management
OA	Office of Administration
OCA	Original Classification Authority
OHS	Office of Homeland Security
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ORCON	Originator Controlled
OSWER	Office of Solid Waste and Emergency Response
PCL	Personnel Security Clearance (or Personnel Clearance)
PI	Preliminary Inquiry
PIN	Personal Identification Number
PL	Protection Level
PR	Periodic Reinvestigation
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
SSBI	Single Scope Background Investigation
SSO	Special Security Officer
SSP	System Security Plans
STE	Secure Terminal Equipment
SVTS	Secure Cellular and Satellite Telephone
TA	Terminal Administrator
TS	Top Secret
U	Unclassified
U.S.C.	United States Code
UK	United Kingdom
VAL	Visit Authorization Letter

This page is intentionally blank

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.) 13526 "Classified National Security Information", dated December 29, 2009; hereinafter referred to as E.O. 13526
- Information Security Oversight Office (ISOO) directive "Classified National Security Information", Final Rule, dated June 28, 2010; hereinafter referred to as 32 C.F.R. 2001
- Executive Order 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. These will be used in evaluating 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 have 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)

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 employee 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 ISOO, on NSI matters
   - Provide reports and costs to ISOO in accordance with EO 13526 and 32 CFR

3. Administrator's Office, EPA (AO/OHS) shall:
   - Determine if EPA personnel requesting SCI access have a requirement and a valid need-to-know
   - Determine if a program office or region has a valid need for the build out of a SCIF or a secure facility
   - Determine if a program office or region has a requirement for installation of the Joint Worldwide Intelligence Communications System (JWICs) the Homeland Secure Data Network (HSDN), and Secure Video Teleconference Systems
   - Review proposed documents for original classification decisions, schedule classification decision meetings with the OCA
   - Review proposed Classification Guides for submission to the OCA for approval
   - Review of classification challenges received by EPA

4. The Director, Security Management Division (Director, SMD) shall:
   - Administer all matters related to the NSI Program

- Implement 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:
   - Provide support and oversight
   - Conduct Inspections of Program Offices and Regions
   - Develop NSI Program policies and procedures
   - Develop and maintain an NSI education and training program
   - Develop and implement the self-inspection program
   - Conduct and review preliminary inquiry (PI) reports
   - Maintain all reports including statistical reports
   - Review and process requests for Mandatory Declassification Review
   - Maintain all original classification decisions made by the OCA
   - Maintain the master EPA security classification guide(s)

6. The NSI Representative shall:
   - Have a minimum of a Secret Security clearance, may require Top Secret clearance for oversight of secure rooms
   - Implement local NSI security training and awareness program to ensure personnel are aware of their responsibilities
   - Conduct an annual self-Inspection of their area of responsibility
   - 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
   - Ensure Drawer Inventory logs are utilized and updated as needed for each drawer of a security container
   - Complete and forward, to the NSI Program Team, all reporting requirements each fiscal year
   - Ensure accountability records are maintained
   - Manage classified visit procedures within their area of responsibility
   - Develop standard operating procedures (SOPs) tailored to the NSI Handbook
   - Disseminate new NSI Program requirements to all pertinent employees
   - Coordinate NSI Program requirements and SOPs covering all classified operations in there program office or region with the NSI Program Team

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 recurrence.

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. 13526, 32 C.F.R. 2001, or this handbook
     - Creates or continues a Special Access Program contrary to the requirements of E.O. 13526
     - The ISOO Director shall be notified when a violation occurs when the violation is reported to oversight committees in the Legislative branch; may attract significant public attention; involves large amount of classified information; or reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.
   - Security Infraction: Any unintentional action contrary to the requirements of E.O. 13526, 32 C.F.R. 2001, 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 NSI Program Team and/or Director, SMD if the circumstances of the incident make it impractical to notify the NSI Representative, supervisor, or next successive supervisor thus ensuring proper security
   - Under no circumstances are individuals authorized to report security incidents to Agencies/Departments outside EPA

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 the security incident
     - Using the format provided in Appendix B, the assigned individual shall forward the PI 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 the 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, SMD 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, an investigator will be appointed 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 OA, 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 32 C.F.R. 2001.

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 October 15th of each year.

3. The NSI Program Team is responsible for completing the SF 311, Agency Security Classification Management Program Data, to ISOO, for the information's inclusion in a report presented by ISOO to the President. The SF311 is a data collection form completed by executive branch agencies that create and\or handle classified information national security information.

4. Information on the costs associated with the implementation of the Executive Order will be collected and submitted to ISOO. ISOO will report these cost estimates annually to the President. The senior agency official shall work closely with the agency comptroller to ensure that the best estimates are collected.

5. The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under E.O.12829, as amended, *National Industrial Security Program,* and consistent with agreements entered into under section 202 of E.O. 12989, as amended, will collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO annually. ISOO will report these cost estimates annually to the President.

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 October 15th of each year. The NSI Representative will maintain a copy of the checklist for two years. The Self Inspection Checklist covers the following topics to evaluate the adherence the principles, requirements, and effectiveness of their NSI program:

- NSI Management
- Security Incidents and Reporting Requirements
- Classification Management (track all original and derivative classifications)
- Classification Markings
- Safeguarding
- Storage
- Destruction
- Transmission Methods
- Education and Training

- Industrial Security Program

Reviews of representative samples of original and derivative actions must encompass all program offices/regions that generate classified information. The review shall include a sample of different types of classified information (document and electronic format such as e-mail).

1-602 Assessment Visits

The NSI Program Team shall continue to conduct periodic assessments of the NSI Program in the Programs and Regions as necessary. These will take place in addition to Inspections as discussed in Section 1-603, to 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
- A review of original and derivative classification actions
- A review of any concerns needed to correct misclassification actions
- Interviews with producers, users, and managers of classified information
- Training will be provided based upon deficiencies noted during the visit

1-603 Inspections

The NSI Program Team shall conduct periodic inspection visits of the Programs and Regions. The inspection cycle is expected to occur on a three year cycle and shall include:

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

Section 7: Emergency Release of Classified National Security Information

1-700 Emergency Release of Classified National Security 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
     - Safeguarding measures should include a discussion on the appropriate methods, and the location of materials designated, for packing and wrapping classified information as noted in Chapter 6, Section 6-300
   - 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 by utilizing a EPA Form 1550-5, Classified Information Chain of Custody Record a sample is provided in Appendix M
   - Provide appropriate briefings to the recipients on their responsibilities not to disclose the information, and obtain a signed SF 312, Classified Information Nondisclosure Agreement
     - In emergency situations requiring immediate verbal release of information, the signed SF 312 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 SF 312s

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

Classified National Security Information is information that has been determined pursuant to E.O. 13526 or any predecessor order, to require protection against unauthorized disclosure, and is appropriately marked to indicate its classified status when in documentary form. Information may be classified in one of two ways, originally or derivatively.

2-201 Classification Standards

1. Information may only be originally classified under the terms of E.O. 13526 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 United States 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. If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:
   - Effect the substantive criteria or procedures for classification
   - Create any substantive or procedural rights subject to judicial review

3. 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, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe

- Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe

- Confidential shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe

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

3. 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.

4. The classification levels of Confidential, Secret, and Top Secret should only be used when identifying NSI.

2-203 Original Classification Authority

1. The President designated Original Classification Authority (OCA) to selected officials to classify information in the first instance. In his December 29, 2009 Implementation memorandum to Agency Heads on EO 13526, the President designated the Administrator, EPA, the authority to originally classify information, at the Secret or Confidential level. Additionally, the President instructed that the Administrator of EPA may not delegate this authority to any other EPA official. The authority to declassify or downgrade information originally classified by EPA may be exercised only by the Administrator, EPA.

2. All OCAs require periodic training at least once per calendar year and can have their authority suspended if the training is not completed.

3. 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 shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with EO 13526 section 1.2, and it pertains to one or more of the following:
   (a) military plans, weapons systems, or operations
   (b) foreign government information
   (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology
   (d) foreign relations or foreign activities of the United States, including confidential sources

(e) scientific, technological, or economic matters relating to national security
(f) Unites States Government programs for safeguarding nuclear materials or facilities
(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security
(h) the development, production, or use of weapons of mass destruction

2. It is expected that most of the information classified within EPA will be categorized by (e) or (g) above.

2-205 Limitations and Prohibitions

1. Classified information that has been declassified without proper authority, as determined by an OCA with jurisdiction over the information, remains classified and administrative action shall be taken to restore markings and controls, as appropriate.

2. A determination that information is classified through the compilation of unclassified information is a derivative classification action based upon existing original classification guidance. If the compilation of unclassified information reveals a new aspect of information that meets the criteria for classification, it shall be referred to the OCA with jurisdiction over the information to make an original classification decision. 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
   - A classified addendum shall be used whenever classified information constitutes a small portion of an otherwise unclassified document
   - If use of a classified addendum is not practicable, derivative classifiers must prepare a separate product to allow for dissemination in unclassified form

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 4-300.

3. The procedures identified below will be followed for submitting the proposal package for review and forwarding to the OCA.

- The NSI Program Team will review the proposal package for compliance with E.O. 13526 and the EPA NSI Handbook. The team will work with the originator and check for:

    - Compliance with classification requirements
    - Proper page and portion classification markings
    - Proper classification block on front cover/page

- The NSI Program Team will forward the document to the Office of the Administrator/Office of Homeland Security (AO/OHS) who will review the proposal and prepare a recommendation memorandum for the OCA. They will also schedule a classification decision meeting with the OCA and, if possible, the originator of the proposal or a subject matter expert

4. 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.

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 establish a specific date or event for declassification based on the duration of the national security sensitivity of the information
    - If unable to determine a specific date or event, the OCA shall attempt to establish a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction
    - 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. If an OCA with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

5. An OCA with jurisdiction over the information may change the level of classification of information. Documents shall be remarked with the new classification level, the date of the action, and the authority for the change. Changing the classification level may also require changing portion markings for information contained within a document. Additionally, the OCA shall update appropriate security classification guides.

2-208 Security Classification Guides

1. Originators of classification guides should consult users for input when developing or updating guides. When possible, originators of classification guides should communicate within their agencies and with other agencies that are developing guidelines for similar activities to ensure consistency and uniformity of classification decisions. The NSI Program Team will provide a template for classification guides, and will maintain a list of all classification guides in use within EPA.

2. Original classification decisions shall be incorporated into a classification guide.

3. Security classification guides shall:
   - Identify the subject matter of the classification guide
   - Identify the OCA by name and position, or personal identifier;
   - Identify an agency point-of-contact or points-of-contact for questions regarding the classification guide
   - Provide the date of issuance or last review
   - State precisely the elements of information to be protected
   - State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified
   - State, when applicable, special handling caveats
   - State a concise reason for classification
   - Prescribe a specific date or event for declassification

4. 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. 13526. 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.

5. 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.

6. Guides will 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.

7. 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.

8. Classification guides will be cancelled only when all information specified as classified by the guide has been declassified.
.

2-209 Declassification Guides

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

2. Declassification guides shall:
   - Identify the subject matter of the declassification guide
   - Identify the original declassification authority by name or personal identifier, and position
   - Provide the date of issuance or last review
   - State precisely the categories or elements of information:
     - To be declassified
     - To be downgraded or
     - Not to be declassified
   - Identify any related file series that have been exempted from automatic declassification
   - To the extent a guide is used in conjunction with the automatic declassification provisions, state precisely the elements of information to be exempted from declassification

3. The SME from the program office or facility is responsible for development of a declassification guide. The guide must be submitted in final draft form to the NSI Program Team.

4. The NSI Program Team will submit the declassification guides for review to ISOO.

5. Declassification guides will be reviewed and updated as circumstances require, but at least once every five years. The NSI Program Team will maintain a list of declassification guides in use.

2-210 Reclassification of Information

In making the decision to reclassify information that has been declassified and released to the public under proper authority, the EPA Administrator must approve, in writing, a

determination on a document-by-document basis that the reclassification is required to prevent significant and demonstrable damage to 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 and the National Security Advisor 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

2-211 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. 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. The duration of the original classified decision shall be placed on the Declassify On line. 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 the downgrading decision.

2-212 Classification Challenges

1. Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established. An authorized holder is any individual, including individuals external to the agency, who have been granted access to specific classified information.

2. At no time will an individual who challenges a security classification be subject to retribution.

3. Classification challenges shall be considered separately from Freedom of Information Act (FOIA) or other declassification requests.

4. 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.

5. Authorized holders shall coordinate classification challenges with the NSI Program Team. 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. The OCA who has jurisdiction over the information will have final determination over the challenge.

6. Classification challenge requests shall be submitted to:
   U.S. Environmental Protection Agency
   National Security Information Program Team
   1200 Pennsylvania Ave, NW
   Mail Code 3206R
   Washington, DC, 20460

7. 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.

8. 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; NSI Program Team shall coordinate classification challenge appeals to the Interagency Security Classification Appeals Panel (ISCAP)

     - Records of challenges shall be subject to oversight by ISOO's,

   - The NSI Program Team shall ensure that each challenge is forwarded to EPA's Office of Homeland Security for an impartial review and processing by the 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 their appeal rights

9. 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.

Section 3: Derivative Classification

2-300 Derivative Classification Principles

1. Derivative classification is reproducing, extracting, or summarizing 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 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. Derivative classifiers must be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification decision.

5. When information is derivatively classified based on "multiple sources" (i.e., more than one security classification guide, classified source document, or combination), the classification block will reflect “Derived From: Multiple Sources”. The derivative classifier must compile a list of the sources used. The derivative classifier shall include a listing of the source materials on, or attached to, each derivatively classified document.
   - Use of a classified addendum shall be used whenever classified information constitutes a small portion of an otherwise unclassified document
   - If use of a classified addendum is not practical, derivative classifiers must prepare a separate product to allow for dissemination in unclassified form

6. A document derivatively classified on the basis of a source document that is itself marked ‘‘multiple sources’’ shall cite the source document on its ‘‘Derived From’’ line rather than the term ‘‘multiple sources.’’

7. 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.

8. 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 whom the originating activity was a part is responsible for determining the action to be taken with respect to classification.

Section 4: Dissemination Control Markings

2-400 Dissemination Control Markings

1. Dissemination Control Markings identify the limitations on the distribution of NSI. These markings are in addition to and separate from the levels of classification defined by E.O. 13526. If used in a document, Dissemination Control Markings are displayed after the classification level, separated by a slash.

2. Common Dissemination Control Markings include "Authorized for Release To", "Not Releasable to Foreign Nationals", and "Originator Controlled".
   - 'Authorized for Release To' (REL TO or REL): Identifies classified information that is releasable or has been released to the foreign country or countries indicated
     - When using REL TO the country code USA must be listed first in REL TO banners for US documents. Following USA trigraph codes for other authorized countries shall be listed in alphabetical order with each code separated by a comma and a space
     - Specific portions of a document, as defined in Chapter 4, Section 4-201, shall be appropriately marked with the designation "REL" when information contained within is authorized for release. An example of each follows:

       Banner Example: SECRET//REL TO USA, CAN, ISR
       Portion Marking Example: (S//REL) These samples are classified for informational purposes only

   - "Not Releasable to Foreign Nationals" (NOFORN): Unless otherwise stated in writing, the use of NOFORN on a classified document prohibits the release of information contained within to any foreign national, foreign organization, or non-US citizen
     - The designation NOFORN cannot be used in conjunction with REL TO
     - Specific portions of a document, as defined in Chapter 4, Section 4-201, shall be appropriately marked with the designation "NF" when information contained within is prohibited from release. An example of each follows:

       Banner Example: CONFIDENTIAL//NOFORN
       Portion Marking Example: (C//NF) These samples are classified for informational purposes only

   - "Originator Controlled" (ORCON): Identifies classified information that identifies or would enable identification of classified sources and methods that may easily be neutralized

- Information designated as ORCON may be disseminated within the recipient's organizational headquarters and specified elements within the organization to include contractors working in government facilities
- ORCON designated information may be combined in whole or in part with other briefings or products; provided the briefing or product is presented or distributed only to original recipients of the information
- Dissemination of ORCON designated information outside the intended recipient's organization requires advanced permission, given in writing, by the originator
- Specific portions of a document, as defined in Chapter 4, Section 4-201, shall be appropriately marked with the designation "OC" when information contained within is prohibited from release. An example of each follows:

  Banner Example: TOP SECRET//ORCON
  Portion Marking Example: (TS//OC) These samples are classified for informational purposes only

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, in accordance with Chapter 2, Section 2-203.

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. 13526 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 2-207
   - 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 Sections 3-301 and 3-302
   - Mandatory Declassification Review A system for reviewing classified information for possible declassification in response to a request that meets the requirements under the Freedom of Information Act (FOIA), Privacy Act of 1974, and the provisions of this handbook. Guidance is provided in Section 3-303

Section 3: Declassification Systems

3-300 Automatic Declassification

1. On December 31, 2006, all classified information and records that were more than 25 years old and were determined to have *permanent historical value* under Title 44 of the United States Code, were automatically declassified unless exemption had been granted from Interagency Security Classification Appeals Panel (ISCAP).

2. All classified information or records classified prior to issuance of E.O. 13526 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 sections 3-300 and 3-301.

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. 13526.

4. To delay the automatic declassification of a specific series of records because it almost invariably contains information that falls within one or more of the exemption categories must submit their request to the NSI Program Team at least one year prior to the onset of automatic declassification.

3-301 Automatic Declassification Exemptions

1. The Administrator, EPA, 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, production, 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 or reveal operational or tactical elements of prior plans that are contained in active war plans
   - Reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government or to ongoing diplomatic activities of the United States
   - 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, or infrastructures relating to the national security
   - Violate any statute, treaty or international agreement

2. The exemption proposal shall be submitted to ISCAP at least one year 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

3. 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 President via the National Security Advisor. The information will remain classified while such an appeal is pending.

4. Information or records exempted from automatic declassification shall remain subject to systematic and mandatory declassification review provisions.

5. When an agency uncovers classified records originated by another agency that appear to meet the criteria for referral, the finding agency shall identify those records for referral to the originating agency. Referrals are required to ensure the timely, efficient and effective processing of reviews and requests and in order to protect classified information from inadvertent disclosure.

6. Restricted Data and Formerly Restricted Data are excluded from the automatic declassification requirements until the Restricted Data or Formerly Restricted Data designation is properly removed. When notified that a Restricted Data or Formerly Restricted Data designation is not appropriate or when it is properly removed, the record shall be processed for automatic declassification.

3-302 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, that still requires protection. These records are maintained at NARA.

3-303 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. 13526. The NSI Program Team shall ensure that requests for declassification are processed in accordance with the provisions of those laws.

Procedures

(a) Information subject to mandatory declassification review. All information classified under E.O. 13526 or predecessor orders shall be subject to review for declassification by EPA if:
  (1) 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
  (2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law; and
  (3) the information is not the subject of pending litigation

(b) Information reviewed within the past 2 years. If EPA has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requestor of this fact and the prior review decision and advise the requestor of appeal rights provided under subsection (h) of this section

(c) Mandatory declassification review and FOIA. When a requestor submits a request both under mandatory declassification review and the Freedom of Information Act (FOIA), EPA shall require the requestor to select one process or the other. If the requestor fails to select one or the other, the request will be treated as a FOIA request unless the requested information is subject only to mandatory declassification review

(d) Submission of request. Requests for mandatory declassification review shall be submitted to the following address:

U.S. Environmental Protection Agency
National Security Information Program Team
1200 Pennsylvania Avenue, NW
Mail Code 3206R
Washington, DC 20460

(e) Content of request. Requests for mandatory declassification review shall identify the requested document or information with sufficient specificity to enable EPA to locate it with a reasonable amount of effort. Information that would provide the sufficient specificity would include a document identifier such as originator, date, title, and/or subject, the National Archives and Records Administration accession number, or other applicable unique document identifying number. Broad or topical requests for information on a particular subject will not meet this standard. All requests shall include a correct return mailing address and a statement that the requestor understands that the request may incur processing fees in accordance with subsection (k) of this section

(f) Receipt of request. Upon receipt of a request, EPA shall acknowledge receipt to the requestor within 30 days and make a final determination within one year from the date of receipt

(g) Referral. When EPA receives a mandatory declassification review request for documents in its possession that were originated by another agency, it shall refer the request, the pertinent documents, and a recommendation for action to the originating agency. EPA may, after consultation with the originating agency, inform the requestor of the referral

(h) Declassification and release. EPA shall declassify information that no longer meets the standards for classification under E.O. 13526 and release the information to the requestor, subject to any applicable processing fees, unless withholding is otherwise authorized and warranted under applicable law (i.e., FOIA, Privacy Act, etc.)

(i) Redaction. When information cannot be declassified in its entirety, EPA shall make reasonable efforts to release, consistent with other applicable laws, those declassified portions of the requested information that constitute a coherent segment unless the overall meaning or informational value of the document is clearly distorted by redaction. The specific reason for the redaction must be included for each redaction

(j) Denial of request and appeal. If the request is denied, EPA will provide the requestor with a brief statement concerning the reasons for the denial and inform the requestor of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial. EPA shall normally make a determination within 60 working days following the receipt of an appeal. If additional time is required to make a determination, EPA shall notify the requestor of the additional time needed and provide the requestor with the reason for the extension. EPA shall notify the requestor in writing of the final determination and of the reasons for any denial. If the appeal is denied, EPA shall inform the requestor of his or her final appeal rights to the Interagency Security Classification Appeals Panel (ISCAP)

(k) Fees. In responding to mandatory declassification review requests for classified information, EPA may charge fees in accordance with 31 U.S.C. § 9701 or relevant fee provisions in other applicable statutes

Section 4: National Declassification Center

3-400 Purpose

The National Declassification Center (the Center) has been established as part of the National Archives to streamline the declassification process, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value.

3-401 Responsibilities

1. Under the administration of the Director, National Declassification Center shall coordinate:
    - Timely and appropriate processing of referrals for accessioned Federal records and transferred presidential records
    - General interagency declassification activities
    - The exchange of detailed declassification guidance to enable the referral of records
    - The development of declassification work processes, training, and quality assurance measures
    - The development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies
    - The storage and related services for Federal records containing classified national security information

2. The Administrator, EPA, shall:
    - Provide adequate and current declassification guidance to enable the referral of records
    - Assign agency personnel to the Center with the appropriately delegated authority to review and exempt or declassify information originated by EPA which are contained in record accessioned to the National Archives
    2. Establish a centralized facility and the operations, as appropriate, to conduct internal declassification reviews in coordination with the Center.

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 about the specific protection requirements for the information. All classified information, to include working papers, 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. Date of Origin of Document shall be indicated in a manner that is immediately apparent.

3. 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.

4. 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" where applicable.

5. Portion Marking Each subject line, title, paragraph, subparagraph, section (i.e., classified diagram, map, drawing, etc.) or similar portions 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:
   - 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. Examples of the appropriate portion markings follows:

     1. (U) Example of portion marking following a number
     A. (S) Example of portion marking following a letter

- The portion marking that precedes the subject or title indicates the classification of the subject or title only, not the classification of the document
  - When possible, select unclassified subjects and titles of classified documents
- Portion mark the title of the illustrative information
- 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

6. A Classification Marking Quick Reference Guide has been produced by the NSI Program Team to provide an overview of marking requirements. The guide is available for download at http://intranet.epa.gov/oa/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 Original Classification Authority (OCA) shall be cited by name and position. It may also include an 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. 13526, Section 1.4 and identified in Chapter 2, Section 2-204
   - **Declassify On:**
     - The "Declassify On" line shall include the duration of the original classification decision. The declassification of a document occurs on a specific date or event. The OCA will identify the declassification date/event when originally classifying the document, as outlined in Chapter 2, Section 2-207. When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD. Events must be reasonably definite and foreseeable

4-301 Marking Examples for Originally Classified Information

1. John Smith, an EPA Laboratory Director, 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 present the work and his reasons for needing classification for the duration of the operation to the Administrator, EPA. Once a determination has been made, Smith will mark this decision on all applicable classified research documents as follows:

   Classified By: (OCA name), Administrator, EPA

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), Administrator, EPA
   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), Administrator, EPA
   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), Administrator, EPA
   Reason: 1.4 (e)
   Declassify On: October 10, 2009 (Classification extended on October 10, 2009 until December 1, 2015, by (OCA name), Administrator, and EPA

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):

- **Classified By:**
  - The derivative classifier shall cite a personal identifier such as name, position, and office symbol
- **Derived From:**
  - Derivative classifiers shall identify the title of the classification guidance and/or source document
  - If more than one source document, classification guide, or combination of the two are used, the line shall read "Multiple Sources", with each source identified on a list maintained with the file or record copy of the document
- **Reason:**
  - The reason for the original classification decision, as reflected in the source documents or classification guide, is not required to be transferred in a derivative classification action
  - If included, carry forward the "Reason" as it appears on the source document
- **Declassify On:**
  - Derivative classifiers shall carry forward the date of declassification specified by the original classifier or use the declassification instructions contained in the classification guide from which the classification was derived
  - When more than one date is specified, the date or event for declassification that corresponds to the longest period of time among the sources shall be used
  - When a document is classified derivatively either from a source document(s) or a classification guide that contains one of the following declassification instructions, ''Originating Agency's Determination Required,'' ''OADR,'' or ''Manual Review,'' ''MR,'' or any of the exemption markings X1 through X8, the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document's date or event to be placed in the ''Declassify On'' line

4-401 Marking Examples for Derivative Classification

1. On October 10, 2005, a cleared employee is drafting a memorandum derived from an EPA Classification Guide dated January 1, 2003. The declassification date in the classification guide states that the particular item of classification is to be declassified on January 1, 2013.

   Classified By: (Name and position of cleared employee)
   Derived From: (Name of EPA classification guide) dated January 1, 2003
   Reason: **1.4(g) and 1.4(f)**
   Declassify On: January 1, 2013

2. On October 11, 2003, a cleared employee is drafting a memorandum derived from a Defense Intelligence Agency (DIA) source document (Subject: Funding Problem) dated November 10, 2002. The source document has a declassification date of December 31, 2019.ui

   Classified By: (Name and position of cleared employee)
   Derived From: DIA Memorandum dated November 10, 2002

Subj: Funding Problem
Reason: **1.4(e)**
Declassify On: December 31, 2019

3. On October 12, 2003, a cleared employee is drafting a memorandum derived from a State Department source document (Subject: IT Developments) dated October 5, 1993. The source document has OADR on the "Declassify On" line.

Classified By: (Name and position of cleared employee)
Derived From: State Department Memorandum dated October 5, 1993
Subject: IT Developments
Reason: **1.4(e)**
Declassify 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.

Classified By: (Name and position of cleared employee)
Derived From: Air Force Memorandum dated December 2, 2000
Subject: New Laser Gun
Reason: **1.4(e)**
Declassify 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).

Classified By: (Name and position of cleared employee)
Derived From: Multiple Sources
Reason: **1.4(g) and 1.4(f)**
Declassify On: December 31, 2019

Section 5: Additional Marking Requirements

4-500 Marking in the Electronic Environment

1. Marking national security information in the electronic environment will be marked with proper classification markings including portion marking, overall classification, "Classified By," "Derived From," "Reason" for classification (originally classified information only), and "Declassify On."
2. Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the OCA.
3. When classified information in an electronic environment cannot be marked in the required manner, a warning will be applied to alert users that the information may not be used as a source for derivative classification and provide a point of contact and

instructions to receive further guidance on the use and classification of the information.

a. Classified e-mail messages are prepared and transmitted on classified systems which will display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail will reflect the classification of the header and body of the message, which include the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail.
b. Classified e-mails will be portion marked, each section marked to reflect the highest level of classification.
c. Classification signature block will be portion marked to reflect the highest level of classification.
d. Subject lines will be portion marked to reflect the sensitivity of the information in the subject line itself and will not reflect any classification markings for the e-mail content or attachments. Subject lines and titles will be portion marked before the subject and title.
e. The classification authority block will be placed after the signature block, but before the overall classification marking string at the end of the e-mail.

4-501 Marking Prohibitions

1. Markings 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" shall not be used to identify unclassified information.

4-502 Documents Proposed for Original Classification

Information pending an original classification decision will be safeguarded in a manner commensurate with 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, as prescribed in Section 4-201, and include the date the document was created on the first page.

4-503 Transmittal Documents

Transmittal documents will indicate on their face the highest classification level of any classified information attached or enclosed. If the transmittal document is unclassified, mark it with the appropriate instruction:

Unclassified When Classified Enclosure Removed or
Upon Removal of Attachment, this Document is (Classification Level)

If the transmittal letter contains classified information, it must be safeguarded per the instructions provided and in accordance with the guidelines prescribed in Chapter 5, Section 5-502.

4-504 Files, Folders, and Binders

1. Cover sheets, Standard Form 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 cover sheet shall be used according to the highest classification of the contents. Samples are provided in Appendix E.

2. Cover sheets shall be affixed each time a classified document is handled or when stored in an appropriate container. Except in instances where the document is placed in a folder or binder with other classified material and the appropriate cover sheet, identifying the highest level of classification is affixed to the exterior.

3. If a cover sheet is not available, mark or stamp the files or folders with the highest level of the classified information contained within.

4-505 Classified Working Papers

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

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.

4-506 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. Documents may be marked Unclassified When Classified

Enclosure Removed or Upon Removal of Attachments, This Document is (Classification Level).

4-507 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.

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 markings. 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 of the recording. 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 legible.

4-508 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."**

4-509 Automated Information Technology (IT) Storage Media

1. Computers and storage media (i.e., hard drives, CDs, DVDs, thumb drives, 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.
   - 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)

- If the media to be marked is formatted as a CD or DVD, the standard forms may not be used on the disc, but shall be placed on the outer case. The appropriate markings on the disc shall be printed legibly using a permanent marker

- SF 710 labels are required for use in any accredited space where unclassified and classified computer systems coexist. Sample labels are provided in Appendix E

3. All media in storage containers used for classified information must have the appropriate classification level label affixed.

4. Additional marking requirements for classified information systems are provided in Chapter 10.

4-510 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 4-201.

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)
Declassified On: October 10, 2004

This page is intentionally blank

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 a GSA-approved class 5 or 6 (legal or letter size) security container within accredited areas
   - 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 personnel
   - Ensuring the safeguarding requirements of this handbook

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
   - They have been in briefed and have signed a Classified Information Non-Disclosure Agreement Form (SF-312) agreement
   - They have a valid need to know
   - Need to know is awarded to personnel who require access to classified information in the performance or assistance of authorized governmental functions.

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

All classified information will be controlled via written records or electronic database and accounted for annually by the NSI Representative.

5-401 Classified Document Accountability

1. All classified information including copies originated or received by an office shall be continuously accounted for, individually serialized, and entered into the NSI Representative's Drawer Inventory Log provided in Appendix O. All information recorded on the Drawer Inventory Log must be unclassified.

2. The log shall include the date originated or received, individual serial number, copy number, unclassified title, originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified), and date of each disposition.

3. Classified 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, all documents must be visually inspected to determine possible downgrade, declassification, or required destruction. One complete copy of the Drawer Inventory Log will be forwarded to the NSI Program Team by October 15th, of each year. This requirement includes rooms that are cleared up to the Top Secret level with no inventory; a Drawer Inventory Log must still be submitted stating no classified information is stored in the room.

4. The Classified Information Accountability Record (EPA Form 1350-2), provided in Appendix H, shall be used to record transmission, reproduction, and destruction of all classified information, and shall be maintained for five years Top Secret and maintained two years for Secret and Confidential. It shall also be utilized when classified information is mailed or transferred to another program/region.
   - Stringent control measures shall be in place for all classified information, to ensure the safeguarding of classified information and include external receipts and destruction/dispatch records to ensure that documents are tracked during transmission and destruction

5-402 Return of Classified Information

1. All cleared personnel who no longer require access to classified information shall:
   - Account for all classified information in their possession
   - Prior to transferring classified information; verify that the intended recipient of the information has a valid security clearance, valid need to know, and the ability to properly store the information

- Transfer all classified information through an approved method

Section 5: Storage

5-500 Policy

1. Classified information must be stored under conditions that 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 a secure area as defined in Section 6.

2. A security container or vault shall not bear any external markings, which may reveal the level of classified information authorized, or stored, or the destruction priority in an emergency situation. 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 access roster shall be maintained by the NSI Representative for each security container and/or drawer in their area of responsibility. At a minimum the access roster should include the individual's name and the containers or drawers they may access.

4. 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 through an approved method as defined in Chapter 6, section 4
   - Arrange with another office or the NSI Program Team, to properly store the information
   - Destroy it via an Agency approved method, as defined in Section 8

5. 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 and a valid need-to-know.

6. Weapons, evidence 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 NSI Program Team may determine that 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 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, as defined by the NSI Program Team, 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, and located in a secure area as defined in Section 6

5-503 Combinations and Passwords

1. Access to Combinations
   - Only appropriately cleared and authorized employees shall have access to security container 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 any alternates (if possible) shall be clearly identified on each SF 700, Security Container Information Form, as provided in Appendix E
     - These employees shall be notified immediately 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
   - Combinations shall only be recorded on SF 700s and protected at the level of the container
   - SF 700s shall be redone each time they are opened or the combination is changed. The SF 700s shall remain sealed as to detect any abnormalities
   - 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 shall be maintained for each locking drawer of a security container. The current SF 700 shall be destroyed via approved methods whenever the combination is changed

- The SF 700 shall be stored in a separate locking drawer or security container
  - If the NSI Representative does not have the means to store the combination in this manner, the SF 700 may be forwarded to the NSI Program Team for storage, via approved methods for transmitting classified information. Additional information is provided in Chapter 6
- The SF 700 for Top Secret combinations shall be accounted for, individually serialized, and entered into the Drawer 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 factory combination of 50-25-50 prior to removal from the office space

5. Computer Passwords
   - Passwords to classified networks and stand alone computers shall be protected commensurate with methods used for security container combinations. The password shall be recorded on an SF 700 and stored in a GSA-approved security container. Refer to Chapter 10 for further guidance

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., crypto card, security container, shredder, computer media, printer, desks). Upon completion, SF 701s shall be retained for a period of three months by the NSI Representative.

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 security container and open storage area to record each time the container/area is locked or unlocked, and shall be used as an end of day check in addition to the SF 701. Once the entire form has been filled, the SF 702 shall be retained for a period of three months by the NSI Representative.

2. The individual who conducts the end-of-day check must ensure the security container and/or door is secure by pulling on the handles. 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 and/or door during the duty day.

3. Reversible magnetic OPEN-CLOSED signs, or similar signs, shall be used as reminders on all classified security containers and secure rooms, when applicable, 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 reviewing, discussing, storing, processing, and destroying classified NSI. Secure areas are defined as follows:
   - Open Storage Accredited Areas
     - Areas used for the continuous review, discussion, storage, processing, and destruction of classified information
   - Secure Accredited Area
     - Areas used for the non-continuous review, discussion, storage, processing, and destruction of classified information

2. Official accreditation by the NSI Program Team is required prior to classified operations beginning for both open storage and secure areas.

3. Accreditations shall be conducted in accordance with Section 5-601 and approved by the NSI Program Team:
   - Accreditations are valid for one year after initial accreditation; thereafter recertification of the room is due annually, by the NSI Representative, to remain in use for classified operations
   - The NSI Program Team may impose more stringent standards if conditions and circumstances are warranted following a risk assessment

5-601 Accreditation Procedures

The following procedures shall be applied to obtain an accreditation of an Open Storage or Secure Area. Construction of the location is dependent upon multiple things including, but not limited to, location of room, windows if any, number of doors, and sound attenuation to determine the type of build out required to obtain accreditation for classified operations:

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. Upon receiving accreditation the NSI Representative shall draft a Standard Operating Procedure (SOP) that details the classified operations approved for the room. The NSI Representative is also responsible for ensuring that the SOP is clearly defined and all occupants receive proper training. The NSI Representative shall provide the room's occupant with a copy of both the SOP and accreditation documentation.

2. Recertification Open storage and secure areas require recertification on an annual basis. The NSI Representative will request recertification of all accredited areas in their area of responsibility by completing Section A of the Accreditation Status Form, provided in Appendix G, and forward it to the NSI Program Team. In addition to submitting an Accreditation Status Form, the NSI Representative shall also submit a Classified Equipment Form, provided in Appendix L, detailing any classified equipment found in the room, or stating that no equipment is installed in the secure room. 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. Change An updated Classified Equipment Form shall be submitted prior to adding equipment or after removing equipment. To add another classified operation, the Accreditation Status Form must be submitted to the NSI Program Team for review and approval. Once approved the NSI Representative will be notified that the new operation can begin. The classified operation is not to take place until the NSI Representative receives approval from the NSI Program Team. To request a change in the classification level or accreditation type (i.e. closed storage to open storage) of a secure room, a Room Accreditation Checklist Form must be submitted by the NSI Representative to the NSI Program Team. After review and approval, a new accreditation letter will be issued to the NSI Representative accrediting the room at the desired classification level and/or accreditation type. Until the new accreditation letter is received by the NSI Representative classified operations must continue at the level indicated in the original accreditation letter.

4. Suspension If the NSI Representative determines classified information might be compromised or that the security conditions are unsatisfactory, they will immediately suspend the accreditation, complete the appropriate information in Section A of the Accreditation Status Form, and forward it to the NSI Program Team. Suspension of an accredited area may also occur when an NSI Representative fails to apply for recertification within a timely manner. Suspension for an accredited area is set to begin one day after the year anniversary of the date on the initial accreditation. A suspended accreditation means that no classified operations can take place until necessary corrections have been made and the area is recertified:
   - Once suspended, all classified equipment must be transferred immediately to another accredited area using an approved method. The NSI Representative shall provide a list of all equipment and where the equipment is being transferred, to the NSI Program Team
   - 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 by the NSI Representative requesting recertification of the area
   - The NSI Program Team will recertify the area by completing the appropriate information in Section B of the Accreditation Status Form and return it to the NSI Representative authorizing recertification. The NSI Representative shall ensure that the room's occupant receives a copy

5. 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, 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 of the withdrawal and verify all classified equipment and information has been removed from the area.

5-602 Open Storage Accredited Area

Open Storage Accredited Areas are used for continuous handling, storing, reviewing, discussing and processing of classified information up to and including Top Secret. Minimum security requirements are listed below, detailed specification is in Appendix N:

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
   - A visitors log shall be maintained to account for all visitors to 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 square 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 sounds 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 door seal 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. The IDS activation/deactivation panel shall be installed within the room and have an established monitoring location. The Premise Control Unit must be installed inside the secure room.

4. 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. The NSI Representative or NSI Program Team will determine an area's sound attenuation by conducting a sound test in the vicinity of all entries/exits located within the room. Where applicable, the sound attenuation test shall be conducted with installed sound masking equipment activated

5. 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 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, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740

6. 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 of the space for discussion

7. Classified Processing:
   - Classified computer processing is authorized, provided the computer has been approved under the National Security Systems Program policy defined in Chapter 10

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 a GSA-approved class 5 or 6 (letter or legal size) security container. Minimum security requirements are listed below, detailed specification is in Appendix N

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. The NSI Representative or NSI Program Team will

determine an area's sound attenuation by conducting a sound test in the vicinity of all entries/exits located within the room

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 personnel responding within 15 minutes of the alarm activation
  - 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

4. Secure Phone:
   - Secure phones are obtained from OSWER and are authorized for use at the classification level of the accreditation of the space for discussion

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

Section 7: Reproduction of Classified Information

5-700 General

This section outlines the security precautions necessary to protect classified 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 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 their area of responsibility.

2. 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.

3. The remote diagnostic capabilities of many classified copy machines shall be disabled and/or disconnected to preclude any internal memory being accessed remotely.

4. Those machines that contain memory capabilities shall have the memory removed by an authorized person prior to servicing by non-cleared personnel.

5. After designation of a copy machine as "approved" or "non-approved," it will be clearly identified by a posted notice.

6. 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 classified information is reproduced, the additional copies must be accounted for in the NSI Representative's Drawer Inventory log.

5-702 Procedures

The NSI Representative shall outline procedures for the reproduction of classified information within their area of responsibility; in addition to the guidelines provided below:

1. Cleared individual(s) shall remain at the copy machine until classified reproduction is complete. Prior to leaving, the machine shall be checked to ensure all originals and copies have been removed.

2. 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.

3. The NSI Representative shall be notified of all service visits 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 NSI Representative. Classified hardware requiring destruction should be forwarded to the NSI Program Team as defined in Chapter 6, section 4:
    - No maintenance personnel shall be allowed unescorted access to any 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 their area of responsibility. These procedures shall ensure only authorized destruction methods are used, and where applicable, that the witnessing and documentation of destruction is completed in an appropriate fashion (i.e., destruction of Top Secret classified information). All destruction of Top Secret classified information shall be documented on EPA Form 1350-2, which will be retained by the NSI Representative for a period of two years:
   - All classified information destroyed via approved methods no longer need be safeguarded by the methods outlined in this chapter

2. 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 NSA-approved crosscut shredders, currently listed on the National Security Agency (NSA/CSS) 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 an authorization certificate by the NSI Representative.

5-802 Unauthorized Destruction Methods

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

This page is intentionally blank

Chapter 6: TRANSMISSION METHODS

Section 1: Overview

6-100 Overview

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

Section 2: General

6-200 Requirements

1. Classified information shall be transmitted and received in an authorized manner that 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 Chapter 5.

2. Classified information shall only be transmitted electronically over approved secure telephones, secure facsimile machines, or approved classified information systems.

3. The NSI Representative will ensure that only appropriately cleared personnel or authorized couriers transmit, transport, escort, or hand-carry classified information. Unless a specific form of transmission or transportation is restricted, 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. Prior to transmitting classified information, the EPA Form 1350-2, Classified Information Accountability Record, provided in Appendix H, shall be completed by the individual transmitting the document and/or package.
   - 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
   - A suspense copy shall be kept by the NSI Representative and subsequently replaced with the original once signed by the recipient

6. Acknowledgement of receipt is required for classified information transmitted, transported, or hand-carried in and out of EPA controlled areas.

Section 3: Packaging for Transmission

6-300 Packaging Requirements for Mailing and Couriering outside EPA Controlled Space

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. EPA Form 1350-2 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.

5. Never leave classified unattended at a United Parcel Service or Federal Express drop off boxes, it must be handed directly to the courier.

Section 4: Methods of Transmission

6-400 Top Secret Information

1. Before transmitting Top Secret information, the sender must coordinate with their 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
   - 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.

6-401 Secret Information

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

- Any of the methods established for Top Secret information
- 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 appropriate to the classification level of the information to be transmitted and detailed in this Section.

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.
   - The courier must ensure the information will not be opened or viewed by customs, border, postal, or other inspectors, regardless of nationality
   - The courier must travel aboard a U.S. carrier
     - Foreign carriers can only be used when no U.S. carrier is available and the courier must receive prior written authorization
   - The courier must ensure that the information remains in their custody and control at all times

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 provided the information is adequately protected against visual observation (i.e., inside a folder, envelope, or briefcase).

2. Classified information shall be double wrapped and transported to preclude unauthorized individuals from reading or accessing the information while it is being couriered between EPA controlled spaces. (i.e., couriering between the Ronald Reagan Building and Ariel Rios North of EPA Headquarters or other Agencies, departments, and facilities).

3. The NSI Program Team Leader is the agency approving official for federal and non-federal personnel to be couriers of classified information. The courier must be appointed by their supervisor, hold an appropriate security clearance, be trained on courier procedures, sign a courier agreement, and possess a valid courier authorization card.

4. As a last resort, classified information may be hand-carried out of the local area, defined as 75 miles from your designated work location, via personal vehicle or aboard commercial transportation methods. These options are to be used in emergency only and when there is neither time nor means available to properly transmit the information by other authorized methods. Prior to departure, the Out Of Area Courier Checklist, provided in Appendix I, is required to be completed by both the courier and the NSI Representative.

5. The NSI Program Team Leader may grant permission to hand-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. The courier card is valid for three years from the date of issue for federal employees and one year for non-federal employees.

4. 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 transportation shall be granted by the NSI Representative in accordance with Section 6-503.

5. 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's discretion.

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.

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 their physical possession at all times
- Prior to hand-carrying classified information, the courier will provide to the NSI Representative a list of all classified information to be hand-carried on a completed EPA Form 1350-2
- 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 via public transportation, or at their home
  - Classified packages shall only be opened in an EPA accredited secure area that has a GSA approved class 5 or 6 (letter or legal) security container
- The courier shall not store classified information in any detachable storage compartment, such as automobile trailers, luggage racks, and aircraft overhead bins when couriering classified information
  - When necessary, packages may be externally inspected or x-rayed (depending upon content) by security personnel when traveling commercially. Couriers must have all documentation and letters of authorization in their possession. No package may be opened by unauthorized personnel regardless of title or designation
- 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 and utilize a EPA Form 1350-5, Classified Information Chain of Custody Form as a means to track the unopened package
- In the event of an emergency, delay, change in destination, loss or compromise of classified information, the courier will immediately notify their NSI Representative or the NSI Program Team
  - If the emergency takes place after standard work hours, the courier will immediately notify the Office of Solid Waste and Emergency Response (OSWER) Emergency Operations Center Watch Officer by calling the telephone number on the courier card
- Emergency contact information is provided on the back of the courier card

6-503 Authorization to Hand-Carry Out of Area via Vehicular or Commercial Transportation

1. Appropriately cleared personnel may be authorized to hand-carry classified information outside their local area or aboard commercial transportation, 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 Commercial Transportation memorandum, sample provided in Appendix I (if applicable)

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

1. Appropriately cleared personnel may be authorized to hand-carry classified information overseas, subject to the following conditions:
   - Written authorization is received 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, regardless of nationality
   - The courier must travel aboard a U.S. carrier
     - Foreign carriers can only be used when no U.S. carrier is available and prior written authorization is received
   - The courier must ensure that the information remains in their custody and control at all times

2. The NSI Representative shall brief the courier concerning security safeguards while couriering overseas and the need to possess EPA photographic identification.

This page is intentionally blank

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 (NSI).

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 Program Team is available to provide support, materials, or training, as required.

3. The NSI Representatives shall provide required security education and training to employees assigned within their Program Offices and Regional locations.

4. 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 Agency employees 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 or the NSI Program Team shall administer initial orientation training.

3. At a minimum, the initial orientation shall address:
   - Roles and responsibilities
     - Senior Agency Official
     - Security Management Division
     - NSI Program Team
     - 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 un-cleared 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 SF 312, Classified Information Nondisclosure Agreement
   - 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 log the receipt of the SF312s and 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. If the appropriate training has not been received in that time, the role must be removed from the agency personnel.

7-401 Original Classification Authority

The OCA will receive original classification training from the NSI Program Team on an annual basis. If the OCA does not receive the mandatory training at least once within a calendar year they shall have their classification authority suspended until the training is completed. At a minimum the OCA training provided shall address the following:

- Differences between original and derivative classification
- Proper safeguarding of classified information
- Administrative sanctions for failure to properly classify information
- Standards that the OCA must meet to classify information
- Discretion that the 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 Derivative Classification

EPA employees who derivatively classify information shall receive derivative classification training no less than once every two years. Derivative classifiers who do not receive such mandatory training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received such training. At a minimum, this training will cover the following topics:

- Principles of derivative classification
- Classification levels, duration of classification
- Identification and markings
- Classification prohibitions and limitations
- Sanctions
- Classification challenges
- Security classification guide
- Information sharing

7-403 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

7-404 Courier Training

1. The NSI Representative or NSI Program Team 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 and responsibilities
   - Emergency situations

3. Administrative procedures for the issuance of a courier card are detailed in Chapter 6, Section 6-501.

7-405 Other Types of Training

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

- 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 annual refresher training is administered as a computer based training to all cleared employees and non-federal personnel. The NSI Representatives are responsible for notifying, and verifying all cleared employees take the annual refresher training.

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. If the refresher training is not taken, the clearance shall be administratively withdrawn.

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 an SF 312, Classified Information Nondisclosure Agreement
   - Mail the originally signed SF 312 to the NSI Program Team
   - The NSI Program Team will log receipt of the SF 312, and will forward the SF 312 to OARM’s Personnel Security Branch to retain in the employee’s security personnel file

This page is intentionally blank

Chapter 8: FOREIGN GOVERNMENT AND NORTH ATLANTIC TREATY ORGANIZATION INFORMATION

Section 1: Overview

8-100 Overview

This chapter defines the principles, standards, and concepts required for safeguarding information classified by foreign governments; including the establishment and identification of the roles and responsibilities, standards, guidelines, and procedures for handling information related to North Atlantic Treaty Organization (NATO) classified information within the U.S. Environmental Protection Agency (EPA). It is applicable to all EPA employees and non-federal personnel that have a requirement to access NATO related information and material in the performance of their duties.

8-101 Authority

- E.O. 13526, "Classified National Security Information", dated December 29, 2009
- 32 C.F.R. 2001, "Classified National Security Information", Final Rule, dated June 28, 2010
- United States Security Authority for NATO Affairs (USSAN) Instruction 1-07 "Implementation of North Atlantic Treaty Organization Security Requirements", dated April 5, 2007
- NATO Document C-M(2002)49, "Security within the North Atlantic Treaty Organization" dated June 17, 2002

8-102 NATO Policy

Consistent with relevant laws, Executive Orders, and Presidential directives all EPA personnel with duties requiring the use of NATO classified information must adhere to the standards and guidelines outlined in, and Standard Operating Procedures (SOPs) derived from, this chapter.

Section 2: Program Management

8-200 NATO Roles and Responsibilities

1. National Security Authority (NSA) - Through DoD Directive 5100.55, the Secretary of Defense shall act as and utilize the title "United States Security Authority for NATO Affairs" (USSAN). With the Deputy Undersecretary of Defense providing principle advice on NATO security policy concerns through the Defense Technology Security Administration (DTSA).

2. Designated Security Authority (DSA) - The Deputy Undersecretary of Defense, acting as DSA, addresses policy matters pertaining to NATO Industrial Security concerns.

3. NATO Sub Registry Control - The NSI Program Team shall act as the NATO Sub Registry Control with regards to all NATO classified information. Primary responsibilities include:
   - Maintain a record of individuals authorized to access NATO classified information and at what level of classification
   - Ensure proper clearance is held prior to granting access to NATO classified information
   - Conduct NATO specific indoctrination, annual refresher training, and debriefings along with witnessing the execution of the NATO brief/debriefing agreement for NATO Control Points

4. NATO Control Point - When required and appropriate, the NSI Program Team or NSI Representative shall act as the NATO Control Point for their Program Office or Region, concerning all NATO classified information. Primary responsibilities include:
   - Assign control numbers and track information classified Cosmic Top Secret (CTS), NATO Secret (NS), or NATO Confidential (NC) upon receipt, dispatch and destruction
   - Conduct NATO specific indoctrination and annual refresher training and witness the execution of the NATO briefing agreement for users located within their area of responsibility
   - Conduct debriefings with individuals no longer requiring access to NATO classified information and witness the execution of the NATO debrief agreement

Section 3: Classification Levels and Marking Information

8-300 NATO Classification Levels

1. NATO classified information shall be classified at one of the following levels:
   - Cosmic Top Secret (CTS) shall be applied to information that could result in exceptionally grave damage to NATO if disclosed to unauthorized sources
   - NATO Secret (NS) shall be applied to information that could result in grave damage to NATO if disclosed to unauthorized sources
   - NATO Confidential (NC) shall be applied to information that could result in damage to NATO if disclosed to unauthorized sources
   - NATO Restricted (NR) shall be applied to information that would be detrimental to the interests and/or effectiveness of NATO. NR shall be protected in the same manner as information designated “For Official Use Only”
   - NATO Unclassified (NU) shall be applied to information that does not have a security classification but shall only be used for official purposes

2. NATO classified information which contains United States Atomic information shall be classified and marked ATOMAL.

8-301 Marking Foreign Government Information (FGI)

1. In addition to the marking requirements detailed in Chapter 4, Section 4-201, 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

8-302 Marking NATO Classified Information

1. Classification markings for NATO information shall be appended in accordance with the guidelines set forth in Chapter 4, Section 4-201 and specifically in regards to overall, interior, and portion marking.
   - 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 level of NATO classified information contained within
   - Conspicuous labels are required at the top and bottom of each page with the highest overall NATO classification level of the information contained within the document
   - Each section, part, paragraph and similar portion of a NATO classified document shall be marked to show the highest NATO classification level of information it contains, or that it is unclassified

2. Each document that contains NATO classified information shall bear a classification marking that reflects the highest level of NATO classified information contained within and include the following:
   - The statement “This document contains NATO (level of classification) information” shall appear on the front of the document
   - If the document contains ATOMAL information the statement “This document contains US ATOMIC information (RESTRICTED DATA OR FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation regarding ATOMIC Information, dated June 18, 1964, and will be safeguarded accordingly.” shall appear on the front cover

3. All material that has been marked with a NATO classification designation must be assumed to contain information that has been released to NATO and shall be controlled under the guidelines set forth below.

4. If the classified information does not have a NATO designation affixed, it will be handled under the same guidelines as would normally be prescribed in this Handbook; unless the originator has designated, in writing, the information is intended for NATO.

5. When an Unclassified document contains NR information, each portion shall be marked as outlined above and include the following:
   - The Statement "This document contains NATO RESTRICTED information – protect as 'FOR OFFICIAL USE ONLY'" shall appear on the front cover

Section 4: Protection and Safeguarding of Foreign Government Information

8-400 Protection of Foreign Government Information

1. 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. .

3. This section is not applicable to NATO designated classified information. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions.

8-401 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.''

8-402 Methods for 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. 13526. 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.

Section 5: Handling and Accounting of NATO Information

8-500 Requirements

1. All material that has been marked with a NATO classification designation must be assumed to contain information that has been released to NATO and shall be controlled under the guidelines set forth in Section 8-302. If the classified material does not have a NATO designation affixed, it will be handled under the same guidelines as would normally be prescribed in this Handbook; unless the originator has designated, in writing, the information is intended for NATO.

2. All U.S. classified material that contains the following statement "Releasable to NATO", including reproductions, has been authorized under applicable disclosure policies for release to NATO and may be discussed with the NATO community. Only those reproductions marked for release shall be dispatched to NATO.

3. Newly generated U.S. classified material that contains NATO classified information shall be marked at the highest level of classified information it contains, with the following additions:
   - On the front cover or first page, if there is no cover, "This Document Contains NATO Classified Information" shall be appended
   - Portions containing the NATO classified material shall be portion marked in accordance with the NSI Program Team guidelines stated above
   - Shall be logged and tracked according to guidelines set forth in this Handbook.
   - Declassification instructions shall indicate that the NATO information is exempt from declassification without the prior consent of NATO, citing "Foreign Government Information" as reason for exemption
   - A record shall be kept of NATO source documents, as required for derivatively classified U.S. documents

Section 6: Packaging and Methods of Transmission

8-600 NATO Packaging and Transmission Methods

1. NATO classified information shall be transmitted in a similar vein to U.S. classified information, of a similar classification level, as described in the NSI Handbook, Chapter 6, with the following additions:
   - The inner sealed cover shall be clearly marked with the highest level of NATO classification of the information contained within
   - CTS shall only be transmitted via military or government courier service
   - Information classified NR or NU shall, at a minimum, be transmitted in a single opaque envelope or wrapping. Single-wrapped packages containing NR information shall not be marked to indicate contents are classified
   - Under no circumstances shall NATO classified material be transmitted via commercial carrier. (e.g., FEDEX, UPS)
   - Diplomatic pouch or military couriers shall be used in the event NATO classified information must be transmitted internationally. Couriering of NATO classified information overseas is prohibited

8-601 Foreign Government Information 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.

Section 7: Reproduction of NATO Information

8-700 Requirements

1. Under no circumstances shall CTS be reproduced.

2. NS information may be reproduced if reproductions are marked with identifying copy numbers and the total number of copies made (e.g., "Copy 1 of 5") and a record of the reproductions are logged and tracked.

3. Copiers, facsimile machines and IT systems used to process and reproduce NATO classified information shall be segregated and physically protected to ensure only authorized individuals have access to them.

Section 8: Security of NATO Information

8-800 Personnel Security

The personnel security aspects of NATO require that an individual's personal reliability and trustworthiness meet specified criteria;

1. Security Clearances - All personnel with access to NATO classified material must hold a final security clearance equal to or higher than the highest classification of the NATO classified information, so long as the following are met:
   - Written authorization has been received and is maintained
   - NATO specific training has been received and acknowledged
     - Note that a NATO Personnel Security Clearance (PSC) is not required for access to NATO Restricted information
   - A valid need-to-know as determined by the official having possession or control of the NATO classified information. No individual is entitled to access NATO classified information based solely upon title, position, or level of security clearance
   - Each Program/Region shall identify positions having a requirement for access to NATO classified information, while a record of PSCs granted to individuals with access to NATO classified information shall be maintained by the designated NSI Representative. The record shall include the level, date, and duration of the clearance

- All individuals no longer requiring access to NATO classified information shall have their NATO Personnel Security Clearance Certificate (PSCC) terminated. They shall be briefed on and acknowledge in writing their continuing responsibilities for the safeguarding of NATO classified information

2. Non-NATO Nationals – Access may be granted on a case-by-case basis if access is necessary to support a specified program, project, or contract and *only* for the duration of the specific program, project, or contract so long as the following have been met:
   - NATO PSCC has been granted based on criteria no less rigorous than for a NATO national
   - Prior written consent of the nation or civil/military body that originated the information has been received
   - Access is limited to NS and in accordance with any dissemination limitation markings
   - A security information arrangement or agreement is in place between the Government of the NATO nation providing access to the information and the Government of the nation of citizenship of the non-NATO individual
   - NATO nation providing access to the information shall be willing to provide access to its own classified information of a similar type and classification level to the nation of citizenship of the non-NATO national

8-801 Training Requirements

Security training is a vital aspect to the proper use and protection of NATO classified information. Users deemed to have a need to know for NATO classified information shall complete NATO specific security training prior to access being granted. An Annual Refresher Briefing is also required for all users. Training materials are developed and maintained by the NSI Program Team.

1. Initial User Training – All users must go through an initial briefing prior to taking control of or accessing NATO classified information. Upon completion of the initial training, holders will be required to sign an acknowledgement statement similar to the SF 312, Classified Information Nondisclosure Agreement.

2. Annual Refresher Briefing - At a minimum, an annual refresher briefing shall occur for all users of NATO classified information. This briefing will remind users of their responsibilities for properly safeguarding and maintaining accountability for the material in their possession. Upon completion all users must sign an acknowledgement statement, included with the initial indoctrination acknowledgement, and will be kept by the NSI Representative for record.

Section 9: Storage of NATO Classified Information

8-900 Storage Requirements

The physical security aspects for NATO classified information consist of safeguarding measures established to provide levels of physical security consistent with the threat,

security classification and quantity of NATO classified information to be protected. The minimum standards for protection of NATO classified information can be found in Chapter 5, Section 502 with the following additions:

1. All NATO classified information shall be stored in separate security containers from non-NATO classified information, with ATOMAL classified further segregated from non-ATOMAL.
   - When space is limited, NATO classified information shall be stored in a separate drawer within an approved non-NATO container
   - If space requirements are minimal, NATO classified information may be stored with non-NATO classified information provided it is contained to specific and clearly defined folders

2. NR shall be stored in a GSA approved locked container.

3. NU shall be stored by any means that deter access by individuals not requiring information for official NATO purposes.

8-901 Combinations and End of Day Checks

The minimum requirements for access, protection and maintenance of combinations safeguarding NATO classified information can be found in Chapter 5, Section 503 with the following additions:

1. The combination settings of security locks used to protect NATO classified information shall be maintained and changed only by individuals having that responsibility and an appropriate security clearance.

2. In addition to the minimum change requirements as set forth, security locks used to protect NATO classified information shall be changed every 12 months.

3. End of Day checks for NATO classified information shall be conducted in accordance with Chapter 5, Section 505.

Section 10: Declassification and Release of Foreign Government Information and NATO Classified Information

8-1000 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. This section does not apply to NATO classified information.

8-1001 Declassification of NATO Classified Information

1. NATO classified information is exempt from declassification or downgrading without the prior written consent of NATO, in the absence of other originator instructions, citing the reason "Foreign Government Information".

8-1002 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: Overview

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 as amended, "National Industrial Security Program (NISP)", dated January 6, 1993; herein after referred to as E.O. 12829
- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), dated February 28, 2006
- Federal Acquisition Regulation (FAR), dated March 2005

9-102 Policy

1. E.O. 12829, 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 5220.22-M 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. 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 DD 254, Department of Defense Contract Security Classification Specification, 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 National Industrial Security Program
   - Account each year for the costs within the agency associated with the implementation of the NISP

2. The Director, Security Management Division (SMD), 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 (CO) and/or Contracting Officer's Representative (COR) with the development of the 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 FAR and the NISPOM regarding the safeguarding of classified information
   - Coordinate with the COR 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 certified by the NSI Program Team Leader 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 if the contractor will be retaining classified information at their facility

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 Defense Security Services (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 the classified contract for incorporation into the DD 254
   - Provide assistance and guidance to the CO and the COR, with respect to national 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 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 NISP.

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 that 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 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 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 coordinated with the NSI Program Team. 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, or Us territories 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 as determined by DSS
     - 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 with a visit certification, which includes the reason for the visit and verification of the employee's clearance
   - The COR or the NSI Representative will verify the clearance with the NSI Program Team 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.

This page is intentionally blank

Chapter 10: NATIONAL SECURITY SYSTEMS PROGRAM

Section 1: Overview

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-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) 44 U.S.C. § 3541, *et seq* of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899), dated December 17, 2002
- Office of Management and Budget (OMB) - Circular No. A-130, Appendix III, dated November 28, 2000
- Committee on National Security Systems (CNSS) policies, directives, instructions, and advisory memorandums
- National Institute of Standards and Technology (NIST) SP 800-59 - Guide for Identification of Information Systems as National Security Systems (NSS), dated August 2003
- EPA Delegation 1-6-A, National Security Information (NSI), dated July 28, 2004
- EPA Information Resources Management (IRM) Policy Manual, Chapter 8
- EPA policies and procedures on classified systems
- EPA System Security Authorization Agreement

10-102 Identifying Information Systems as National Security Systems

1. A National Security System (NSS), as defined by the "NIST SP 800-59 Guide for Identification of Information Systems as National Security Systems" 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. EPA NSS may be referred to as "Classified Systems or Classified Information Systems" throughout this chapter.
   - Stand-Alone Classified Computer Systems (Non-Network)
   - Homeland Secure Data Network (HSDN)
   - Joint Worldwide Intelligence Communications System (JWICS)
   - Secure Cellular and Satellite Telephones (SCST)
   - Secure Telephone Equipment (STE)
   - Secure Video Teleconferencing System (SVTC)

3. Sensitive Compartmented Information (SCI) related equipment must comply with Chapter 11 requirements

4. Communication Security (COMSEC) related equipment must comply with Chapter 12 requirements

10-103 Policy

1. All personnel with classified information systems security responsibilities must adhere to the current laws, directives, and regulations for NSS in addition to standards, guidelines, and procedures of this chapter and applicable Standard Operating Procedures (SOPs) when EPA classified information systems are used to support collateral (Top Secret, Secret, and Confidential) classified processing requirements.

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 defined in the paragraphs below.

1. Designated Approval Authority (DAA)
   The Director, Security Management Division (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) and the System Security Plan (SSP). 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 Personnel Security Branch Chief is designated as the ISSM for EPA. The ISSM is responsible for oversight of EPA's NSSP. The ISSM shall:

- Approve NSSP standards, guidelines, and procedures
- Ensure periodic reviews are conducted to ensure the program is effectively implemented
- Ensure an independent evaluation of NSS is conducted and the results reported annually to the 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 applicable federal regulations
- Provide guidance for developing the SSAA, SSP, and Memorandums of Agreement (MOA) for use with classified information systems
- Review SSAAs, SSPs, and MOAs

3. Information System Security Officer (ISSO)
   A staff member of the NSI Program Team is designated the ISSO. The ISSO must 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
   - Write the required SSAAs, SSPs, and MOAs for use with NSS for the agency
   - Provide guidance for the approval of EPA's NSS
   - Draft security awareness and training for EPA's NSSP
   - Conduct periodic compliance reviews by program and region
   - Coordinate with the Information System Security Representatives (ISSR) and System Administrators to ensure proper implementation of approved security features
   - Conduct Preliminary Inquires and Investigations
   - Approve and publish all NSS equipment SOPs
   - Authorize NSS users

4. Information System Security Representative (ISSR)
   The ISSR assists the ISSO 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 must be performed by competent technical personnel and function independently (i.e., separation of duties) from the System Administrator. The ISSR must 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 and SSP
   - Ensure System Owners and System Administrators maintain systems in compliance with the approved SSAA and SSP
   - Conduct audits on installed security features

5. NSI Representatives
   The NSI Representative is responsible for all classified material and equipment within their purview. The NSI Representative shall:
   - Be actively engaged in ensuring that the users are properly trained and authorized to maintain the NSS equipment within their areas and that the equipment is only utilized in accredited spaces or within the guidelines of the SOP for that respective equipment
   - Be informed of any changes to or maintenance of all classified processing equipment within their area
   - Maintain an inventory of all classified processing equipment to include the type, model, serial numbers and names of the system owners for said equipment
   - Comply with the requirements of the SOPs
   - The NSI Representative will maintain a list of all authorized STE users within their area of responsibility to verify access requirements are met, i.e. accredited space, and appropriate level of security clearance

6. System Owner
   The System Owner refers specifically to Stand-Alone Classified Information System Computers and is responsible for the procurement and daily operation of their 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 with a security clearance equal to the highest level of classified information that will be stored or processed on the system
     - EPA HQ shall utilize a NSI Program Team member as the System Administrator
   - 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
   - Ensure the System Administrator implements and maintains the technical controls and configuration guidance listed in the SSAA and SSP
   - Comply with applicable SOPs
   - 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 who have received Initial User Training and have signed the appropriate User Agreement Form are permitted access to classified equipment
   - Formally notify the ISSO when a system is no longer required to process classified information

- Ensure user password is protected at the highest classification level of data on the system and annotate the password utilizing a SF 700, Security Container Information, as outlined in Chapter 5
- Complete the Initial User Training before accessing a system
- Acknowledge the responsibilities for adequately protecting classified systems by signing the appropriate User Agreement Form
- Complete periodic refresher training on the proper use of secure equipment
- Notify the ISSO of any repair or maintenance performed on any NSS

7. 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 and SSP
   - 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
   - Ensure user password is protected at the highest classification level of data on the system and annotate the password utilizing a SF 700, as outlined in Chapter 5
   - Complete the Initial User Training before accessing a system
   - Acknowledge the responsibilities for adequately protecting classified systems by signing the appropriate User Agreement Form
   - Complete periodic Refresher Training for the secure equipment
   - Notify the ISSO of any repair or maintenance performed on any NSS

8. User
   A User must possess a clearance equal to or higher than the highest classification of information stored or processed on NSS. The User shall:
   - Comply with the requirements of the SSAA
   - Comply with the requirements of the SOPs
   - Be aware of and knowledgeable of responsibilities regarding classified system security
   - Be accountable for his/her actions while using the classified information system
   - Ensure their User password is protected at the highest classification level of information on the system and annotate the password utilizing a SF 700, as outlined in Chapter 5
   - Complete the Initial User Training before accessing a system

- Complete periodic NSS refresher training
- Acknowledge the responsibilities for adequately protecting NSS by signing the appropriate system specific User Agreement Form
- A system User is also referred to as the Hand Receipt Holder for COMSEC material and must comply with the requirements in Chapter 12 for COMSEC equipment

9. Communication Security (COMSEC) Custodian
   The COMSEC Custodian is responsible for the issuance, maintenance and management of all EPA COMSEC equipment and material. This includes all NSS that utilize cryptographic material. The COMSEC Custodian shall comply with the requirements of Chapter 11 and Chapter 12 and all applicable NSSP SOPs.

Section 3: Program Planning

10-300 Planning Standards

The CNSS National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP) shall be used for NSSP planning and for the certification and accreditation process.

1. Stand-Alone Classified Computer Information Systems
   - System Security Authorization Agreement (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 information system
     - Establishes system-level security requirements, defines operational and technical controls, and establishes access requirements for stand-alone information systems
     - Is used to guide and document the results of certification and accreditation
     - After accreditation, the SSAA becomes the baseline security configuration document
     - The SSAA Master Plan, approved by the DAA, maintained by the NSI Program Team, further defines the registration and certification process
   - System Security Plan (SSP)
     - An SSP 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 information system
     - Establishes system-level security requirements, defines operational and technical controls, and establishes access requirements for Sensitive Compartmented Information (SCI) stand-alone information systems
     - Is used to guide and document the results of certification and accreditation
     - After accreditation, the SSP becomes the baseline security configuration document
     - The SSP, approved by the DAA of the agency with security cognizance over the system, and maintained by the NSI Program Team, further defines the registration and certification process

- Registration and certification process
  - Effective security measures used with stand-alone classified information systems shall include physical, procedural, and personnel access controls to prevent unauthorized individuals from accessing the systems

2. Classified Telecommunication Systems and Other NSS devices
   - Registration and certification, issuing and authorization process
     - All classified telecommunication systems will be vetted through and authorized for use by OSWER in accordance with the NSI Handbook and in coordination with the NSI Program Team

Section 4: Training

10-400 Security Training Requirements

Security training is an essential aspect of the NSSP.

1. Prior to accessing NSS, prospective users must first have received the Initial NSI Orientation Training from the NSI Program Team or NSI Representative and met all of the training requirements outlined in Chapter 7.

2. Users of NSS will complete system specific training prior to being authorized access to that system.

3. NSS users may be required to take periodic refresher training on certain NSS. Any user not participating in required training shall have user logon rights removed or have their access restricted until training is completed.

4. At the completion of all NSS training, users will sign a system specific User Agreement acknowledging they understand and will comply with the proper handling of classified material and the rules and regulations governing the NSS.

Section 5: Operations

10-500 Access

To access an EPA NSS, all personnel must meet the requirements in Chapter 5, Section 3 and must have attended NSS specific training.

1. Contract Management
   All contractors must follow the provisions of the NSI Handbook to be authorized to process information on EPA NSS within EPA facilities.

2. 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 escort personnel.

3. 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 NSSP 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 NSSP policies and procedures of the host department or agency apply
   - If there is a conflict regarding which agency's NSSP policies apply, always use the most restrictive procedures

10-501 Physical Security

The physical security aspects of NSS 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.
   - The unique physical security requirements of classified discussions, while using a SCST in a non-secured area, are addressed within the SCST SOP

2. Storage Requirements
   - Users of classified information 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., thumb drives, floppy disk, Compact Disk/ Digital Video Disc (CD/DVD) must be stored in an approved security container or an accredited open storage area when not in use
   - Users of the SCST and STE must comply with the following storage requirements for the secure telephones, Crypto Cards and PINs.
     - A SCST must be maintained in the possession of the owner or an authorized user at all times, or secured in an approved security container
     - The PIN for the SCST must never be stored in the same location or associated with the telephone at any time until ready to use

- The SCST and the PIN are both unclassified until they are associated with each other (e.g. PIN is entered into telephone)
- A STE must be secured in an accredited room.
- The Crypto Card must secured within an approved security container if it is stored in the same room as the STE
- The Crypto Card may be secured in a locker, cabinet or desk when it is NOT stored in the same room as the STE
- Only authorized STE users are permitted access the Crypto Card storage location
- The STE and the Crypto Card are both unclassified but must be protected at the classification level authorized by the Crypto Card when it is inserted into the STE

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 their security classification. This 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 required (SF 706, SF 707, SF 708 and SF 710). 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.
   - All classified CDs and DVDs will be legibly marked utilizing a permanent marker. Adhesive labels shall not be utilized.
   - Classified CD or DVD Jewel case will be marked with the appropriate classification adhesive label.
   - Classified thumb drives will use the classification adhesive label on the device when possible and will have an attached “tag” which will also have a classification adhesive label.

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 and removable hard drives). The labels should be the same as described above in item 4. If the label impedes operation of the component, permanent markings on the component or a sign placed on the terminal is appropriate.
   - The labeling requirements do not apply to the STE, Crypto Card, or the SCST

6. Protecting Displayed Information
   All users must ensure that the monitor or the telephone display cannot be viewed by unauthorized individuals. 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 Computer Systems, Cabling or Telephones
   The following conditions shall be adhered to when a classified computer is co-located with an unclassified system, cabling or telephone:
   - A computer approved for processing unclassified information, in a classified environment, must be clearly marked as an unclassified computer using the SF 710 unclassified labels
   - A computer approved for processing unclassified information must be physically separated, at least one meter, from any classified computers or NSS
   - 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
   - An unclassified telephone must be physically separated, at least one meter, from any 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 immediately to the NSI Program Team or the DAA
   - 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 NSS require documentation of critical security actions to demonstrate compliance.

1. Access
   All access to a NSS 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 a NSS. Access is only allowed when the following conditions are met:
   - System Owner, System Administrator or NSI Representative has verified the need-to-know
   - System Owner, System Administrator or NSI Representative has verified the user possesses an appropriate security clearance
   - COMSEC Custodian has verified the user possesses an appropriate security clearance, when applicable
   - All applicable training requirements have been completed
   - User has signed a system specific User Agreement for access to the NSS
   - The System Owner shall maintain a list of authorized users for each Stand-Alone Computer within their area of responsibility
   - The NSI Representative and the secure telephone owner will maintain a list for all authorized users of all secure telephones within their area of responsibility
   - The COMSEC Custodian will maintain a list of all owners of secure telephones as well as all personnel issued all other cryptographic equipment

- The NSI Program Team shall maintain a list of authorized users for all NSS

2. User Agreements for NSS
   The 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 all required training. Access to the NSS will only be granted after the agreement is signed.

3. System Owner's Manual
   The system owner shall maintain a Systems Owner's Manual or a comparable filing management system with each Stand-Alone Classified Computer under their area of responsibility.

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. The 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) or PIN 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 PINs, Code Words and Combinations. The following shall be adhered to in conjunction with the provisions of Chapter 5, Section 5:
     - Shall be protected at a level commensurate with the classification of the information to which they allow access
     - Utilize the password generation method (e.g., password length, character set) as described in the SSAA
     - COMSEC Custodian may assign PINs for COMSEC equipment
     - Shall be annotated on an SF 700 for each user and for each individual item
     - All SF 700s shall be stored in an approved security container commensurate with the system. The NSI Program Team can provide an alternate storage facility for the SF 700s as needed

5. Malicious Code Prevention
   NSS 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., thumb drives, 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 without the authorization of the ISSO
   - Owners or users of the STE or SCST will not download or attempt to download any software into the telephones

6. Printing Protection
   Users must use only an authorized classified and properly marked printer. 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 NSS System Owner or COMSEC hand receipt holder and NSI Representative must maintain a complete and up-to-date inventory of all system components and peripheral devices for all NSS within their area of responsibility.
   - The Stand-Alone Computer System Owner must submit a completed inventory using the Registration/Certification Form to the DAA to obtain the initial approval to operate the system
   - The NSI Representative will be provided a copy of all inventories of NSS within their area of responsibility
   - The NSI Representative will be notified immediately of any changes to the inventory and/or status of all NSS
   - All COMSEC related NSS equipment inventories will be in accordance with Chapter 12

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. Copy the unclassified data onto the media, select the "close portion" option, which prevents any further data being written to the CD/DVD
c. Mark media according to the same classification level as the classified system
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 and equipment. 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
  - Once cleared, the media can only be used at the same classification or higher level as the original data. A cleared device can never be utilized in any system of a lower classification level
  - 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

- All NSS computer and telecommunications equipment will be returned to the NSI Program Team or the COMSEC custodian for all issues regarding, cleaning, sanitizing, declassification or destruction. NSI Representatives, COMSEC hand receipt holders, System Owners or users will not conduct any of these procedures without the direct written authorization of the NSI Program Team or COMSEC Custodian

10. System Maintenance

A NSS is particularly vulnerable to security threats during maintenance activities. Prior to conducting any maintenance, the System Owner will notify the ISSO of planned maintenance, diagnostics or repair to an NSS. 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 otherwise authorized by the DAA
  - Cleared personnel who perform maintenance, diagnostics or repairs on a classified system do not require an escort, unless need-to-know controls must be enforced
- Uncleared or Lower Cleared Maintenance Personnel
  - The escort MUST maintain continuous unimpeded visibility and observation of the personnel, media and systems throughout the entire process
  - 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 within the System Owner's Manual for computer systems
  - 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 NSS 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 ISSO or ISSR
- After maintenance has been performed, the security features on the system shall be recertified

- All telecommunications equipment will be returned to the NSI Program Team or the COMSEC custodian for all issues, maintenance or repairs. NSI Representatives, COMSEC hand receipt holders, System Owners or users will not conduct any of these procedures without the direct written authorization of the NSI Program Team or COMSEC custodian

11. Record Keeping
    - For computer systems, ultimately, the System Owner must ensure that the official records listed below, where applicable, are maintained in the System Owner's Manual or filing system for each NSS 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
    - For all telecommunication systems, ultimately the COMSEC custodian must ensure that the official records for each system and all transactions are properly accounted for and all records maintained

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 October 15th 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 NSS:
   - 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
  - NSS 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 and immediate need required for the 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 applies 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	NOT ALL	Not	High, Med, Basic

	Equal to Highest Data	Users Have ALL	contributing to the decision	

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 with 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 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
   - Integrity
     - Find the column representing the Level-of-Concern for integrity (e.g., Basic, Medium, High) in Table 4
     - The cells in the column directly below the Level-of-Concern are the assurance requirements for the associated technical security feature identified in the associated left column
   - Availability
     - Find the column representing the Level-of-Concern for availability (e.g., Basic, Medium, High) in Table 5
     - The cells in the column directly below the Level-of-Concern are the assurance requirements for the associated technical security feature identified in the associated left column

CONFIDENTIALITY			
	Protection Level Level of Concern (High, Med, Basic)		
Technical Security Features	**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 2]**			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

Section 6: Security Incidents

10-600 Reportable Security Incident (RSI)

1. Unclassified Computer Systems
   If classified information is discovered, loaded, or inadvertently processed on any unclassified computer, the incident will be reported immediately in accordance with EPA's Computer Security Incident Response Capability (CSIRC) procedures and the NSI Program Team for classified spillage notification.

2. Classified Computer Systems
   If classified information is discovered, loaded or inadvertently processed on any classified computer that is not accredited for the level of classified material (e.g. Top Secret material discovered on a Secret machine) the incident will be reported immediately to the NSI Program Team.

3. Reporting
   Immediate reporting is essential to minimize the impact to classified/unclassified systems or networks. Reporting is conducted as follows:

- Immediately report the incident, verbally, to the NSI Program Team, the ISSR and the NSI Representative.
- The ISSR will verbally report to the ISSO and the EPA CSIRC via the EPA Call Center at 1-866-411-4EPA (4372)
- The ISSR will forward a written report to the ISSO and the EPA CSIRC to provide documentation of the incident

4. Unsecured Classified Material
   Any classified material, equipment, or media discovered unattended will be immediately reported to the NSI Representative and the NSI Program team in accordance with Chapter 1.

5. Classified Telephone Systems (STE and SCST)
   The STE and SCST SOPs list specific security incidents called Practices Dangerous to Security and COMSEC Incidents that must be reported immediately to the NSI Program Team and the OSWER COMSEC Custodian. Some examples of these occurrences are:
   - Failure to rekey the telephone, telephone malfunction, expired or compromised key or PIN
   - Utilizing the telephone in the secure mode in the presence of unauthorized personnel
   - Unattended secure keyed telephone or collocation storage of the PIN and telephone
   - Evidence of tampering or unauthorized access to any secure telephone equipment
   - Loss or theft of any secure telephone equipment

Section 7: Emergency Action Plan

10-700 Emergency Action Plan

The NSI Representatives will be responsible to create and publish an Emergency Action Plan for their area of responsibility. The Emergency Action Plan shall:

- Include instructions and procedures to be followed for the proper safeguarding of NSS classified equipment or material in the event of a natural disaster or National Security Threat but not at the risk of loss of life.
- Coordinate with the OSWER COMSEC Custodian to ensure the safe handling or destruction of all COMSEC material in the event of a national event or natural disaster

Section 8: Destruction

10-800 Destruction of NSS Equipment or Material

The destruction of all NSS equipment and material shall be conducted by the NSI Program Team.

- All NSS equipment and material identified for destruction or having exceeded its life cycle or usefulness shall be submitted to the NSI program Team with a request for disposal
- The NSI Program Team will provide the owner a signed EPA Form 1350-2 receipt for the material and will notify the owner upon completion of the destruction
- The destruction procedures are superseded by the Emergency Action Plan, situational dependent

This page is intentionally blank

Chapter 11: Sensitive Compartmented Information Program

Section 1: Overview

11-100 Overview

Sensitive compartmented information is national intelligence information concerning or derived from sensitive intelligence sources, methods, or analytical processes, which is to be handled exclusively within formal access control systems established by the Director of National Intelligence. This chapter covers EPA's Sensitive Compartmented Information (SCI) Program, and the program's policies and procedures.

Section 2: Access Programs

11-200 Policy

1. The granting of access to SCI will be controlled under the strictest application of the need-to-know principle, in accordance with the Intelligence Community Directives, the personnel security standards, and Executive Orders.

2. The NSI Program Team supports the administrative needs of EPA federal and non-federal employees requiring authorization for SCI access.

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 as amended; hereinafter referred to as E.O. 12333, which establishes the Intelligence Community; and the Intelligence Reform and Terrorism Prevention Act (IRTPA) which establishes the Director of National Intelligence (DNI) as head of the intelligence community. The DNI is responsible for protecting intelligence sources, methods, and analytical procedures.

3. Security policies for SCI are documented in Director of Central Intelligence Directives (DCID), Intelligence Community Directives (ICD), and Intelligence Community Policy Guidance (ICPG). The following is a list of DCIDs, ICDs and ICPGs that SCI-cleared EPA employees will most often utilize. (Note: All DCIDs will eventually be replaced by ICDs).
   - DCID 1/19 Security Policy for Sensitive Compartmented Information and Security Policy Manual
   - ICD/ICS 705 - Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities,
   - ICD 503 - Intelligence Community Information Technology Systems Security Risk Management, Certification & Accreditation, dated September 15, 2008

- ICD 701 – Security Policy Directive for unauthorized Disclosures of Classified Information dated March 14, 2007
- ICD 704 - Personnel Security Standards and Procedures Governing Eligibility for Access to SCI And Other Controlled Access Program Information, effective October 1, 2008
- ICPG 704.1 Personnel Security Investigative Standards and Procedures Governing Eligibility For Access to Sensitive Compartmented Information and Other Controlled Access Program Information, dated October 2, 2008
- ICPG 704.2 Personal Security Adjunctive Guidelines For Determining Eligibility For Access To Sensitive Compartmented Information and Other Controlled Access Program Information dated October 2, 2008
- ICPG 704.3 Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information and Appeals Processes, dated October 2, 2008
- ICPG 704.4 Reciprocity of Personnel Security Clearance and Access Determinations, dated October 2, 2008
- ICPG 704.5 Intelligence Community Personnel Security Database Scattered Castles, dated October 2, 2008

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 (IRTPA). 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 of the Central Intelligence Agency and the Office of the Director of National Intelligence. The roles and responsibilities for EPA's SCI program are as follows:

1. Director of National Intelligence (DNI)
   - Determine intelligence pertaining to more than one Government agency
   - Develop guidelines on how intelligence is provided or accessed by the Intelligence community
   - Oversee all ongoing and proposed covert action programs
   - Establish common security and access standards for managing and handling intelligence systems, information, and products
   - Protect intelligence sources, methods, and activities from unauthorized disclosure
   - Declassify, or direct the declassification, information or intelligence relating to intelligence sources, methods and activities

2. Central Intelligence Agency (CIA)
   - Grant authorization for SCI access
   - Maintain a database of all SCI access
   - Accredit 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

3. Administrator's Office, EPA (AO) shall
   - Be responsible for determining if EPA personnel requesting SCI access have a requirement and a valid need-to-know
   - Be responsible for determining if a program office or region has a valid need for the build out of a SCIF

4. Special Security Officer (SSO)
   The NSI Program Team Leader has been 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
   - Process visit requests
   - Maintain required SCI administrative files
   - Conduct periodic reviews of EPA SCIFs

5. SCIF Managers
   Employees at other EPA SCIFs responsible for the oversight and management of a SCIF in their area of responsibility

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 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 Reinvestigation (PRI) 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 J.
   - 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 prior to forwarding to the AO
- 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 attend initial SCI training, program indoctrination briefing(s), and sign the SCI Nondisclosure Agreement, Form 4414.
   - The Form 4414, SCI Nondisclosure Agreement, 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 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 K, to the NSI Program Team at least five working days prior to the intended visit
   - 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 all 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 to the NSI Program Team in writing, any activities, conduct, or employment that may affect their ability to protect classified information from unauthorized disclosure or counter-intelligence threats. A complete list of reporting requirements can be found in ICPG 704.2 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
- SCI cleared individuals must have a Defensive Travel Brief prior to traveling outside the Continental United States whether going on official or unofficial business

- 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) who may be 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. As an application of control, accountability provides a formal mechanism to maintain a constant level of accountability for SCI.

   - SCI Accountability
     - All SCI (including copies) originated or received by an office shall be continuously accounted for, individually serialized, and entered into the SCIF managers Drawer Inventory 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
     - All SCI shall be inventoried annually (with the results compiled by October 15th), at the change of the SSO, and/or upon the report of loss or compromise
       One complete copy of the SCI inventory will be forwarded to the NSI Program Team
     - During the annual inventory, each document must be visually inspected or destroyed to reduce the amount stored for operational and program purposes
     - The Classified Information Accountability Record, shall be used to record transmission, reproduction, and destruction of all SCI and shall be maintained for five years
     - Control measures include external receipts and dispatch records to ensure that documents are tracked during transmission

6. SCI Transmission SCI transmissions shall be accomplished in a manner to preclude loss or compromise. Transmitting SCI must be controlled through authorized transmission methods, and accounted for by use of a Classified Information Accountability Record. 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
  - Designated courier with appropriate SCI access
  - Electronic means over SCI approved communications systems

7. Destruction of all SCI shall be annotated on the Classified Information Accountability Record EPA Form 1350-2 and requires two person integrity when being destroyed

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

Any employee with knowledge of possible or actual security violations, infractions, or compromise involving SCI shall report the incident to the NSI Program Team and supervisor immediately. Further guidance on reporting requirements are provided in Chapter 1, Section 3. If the Director, SMD, determines that an incident is a significant security violation or a compromise has occurred, as defined by ICD 701, CIA shall be immediately notified by the SSO.

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 processed within an accredited SCIF. A SCIF is an accredited area intended to prevent access to SCI by unauthorized persons.

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
     - 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 ICD 705 Fixed Facility Checklist
   - Official accreditation letter
   - Inspection reports for the entire period of SCIF accreditation
   - Operating procedures, 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
- SF 700, Security Container Information Form
- SF 701, Activity Security Checklist
- SF 702, Security Container Check Sheet
- 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, unique ID, purpose of visit, date of visit, signature/printed name of the escort, clearance level 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 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

Contracting Officer's Representatives must ensure that contractors requiring SCI access have incorporated/referenced the requirements established in this handbook within each DD254, Contract Security Classification Specification.

11-306 SCI Security Education

The NSI Program Team shall administer a continuing security education program for all personnel authorized access to SCI. 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 Briefing
     - 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
   - Sensitive Compartmented Information Nondisclosure Agreement Briefing
     - This Agreement identifies the responsibilities of individuals on the protection of SCI from unauthorized disclosure

- Program Specific Briefing
  - This briefing describes the compartments to which access has been granted
- SCI Indoctrination Briefing
  - This briefing describes:
    a. Personal, administrative, and procedural requirements
    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 is 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

3. Defensive Travel Briefing This briefing is designed to provide awareness of security vulnerabilities and personal responsibilities associated with traveling outside the United States.
   - This training is to be administered prior to official and unofficial travel outside the United States, to all individuals possessing SCI access

4. SCI Debriefing The debriefing 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

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 ICD 503.

- The certification and accreditation process includes the approval of a System Security Plan (SSP) written by the system owner
- The NSI Program Team shall:
  - Provide review and assistance with the development of the System Security Plan
  - Coordinate with the appropriate Designated Accrediting Authority

This page is intentionally blank

Chapter 12: COMMUNICATIONS SECURITY (COMSEC)

Section 1: Overview

12-100 Overview

This chapter defines the regulations and responsibilities of the EPA Communications Security (COMSEC) Program while establishing and identifying the roles, responsibilities, standards, guidelines, and procedures for COMSEC within the EPA.

12-101 Authority

- Committee on National Security Systems (CNSS) policies, directives, instructions, and advisory memorandums
- Committee on National Security Systems (CNSS) Policy No. 1, National Policy for Safeguarding and Control of COMSEC Materials, September 2004
- Committee on National Security Systems (CNSS) Policy No. 3, National Policy for Granting Access to U.S. Classified Cryptographic Information, October 2007
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997
- National Security Agency/Central Security Service (NSA/CSS) Policy Manual No. 3-16, Control of Communication Security (COMSEC) Material, August 5, 2005
- EPA Delegation 1-6-A, National Security Information, June 19, 2007
- EPA Order 4850, National Security Information, July 23, 2007

12-102 Policy

Consistent with relevant laws, executive orders, and Presidential directives all EPA personnel, federal and non-federal, with duties requiring the use, operation or maintenance of cryptographic keying material or secure telecommunications equipment must adhere to the standards and guidelines outlined in the NSI Handbook and Standard Operating Procedures (SOP) derived from this chapter.

The NSA/CSS Policy Manual No. 3-16 delineates specific instructions in the Roles and Responsibilities and systematic operations, management and accounting of all COMSEC material within EPA.

Section 2: Program Management

12-200 Roles and Responsibilities

1. The Central Office of Record (COR) Authority - Director, National Security Agency (NSA), shall:
   - Conduct Reportable Inspections of COMSEC accounts every two years
   - Conduct a Reportable COMSEC Inventory every 6 months
   - Supply COMSEC material and information to EPA

2. The Assistant Administrator, Office of Administration and Resources Management (OARM), as the Senior Agency Official (SAO), shall:
   - Ensure the proper administration of the COMSEC Program
   - Immediately notify the Director, NSA, of all compromises of COMSEC material

3. The Director, Security Management Division (SMD), shall:
   - Oversee the management of the COMSEC Program
   - Review Preliminary Inquires and COMSEC incidents
   - Report all security violations to the SAO upon completion of any inquiry

4. The National Security Information (NSI) Program Team, shall:
   - Provide oversight of EPA's COMSEC Program
   - Be the advisor to the Director, SMD on matters concerning the security and handling of COMSEC material and equipment
   - Develop and implement EPA COMSEC policy directives, standards, and procedures
   - Conduct internal inspections, assessments, audits and Preliminary Inquiries of the COMSEC program
   - Report all accounting irregularities, security violations or loss of COMSEC material immediately to the Director, SMD, and recommend immediate action to prevent further loss or compromise of COMSEC material or information
   - Coordinate establishing and closing of all COMSEC accounts

5. The Office of Solid Waste and Emergency Response (OSWER), as the COMSEC Controlling Authority shall:
   - Define new secure data and voice requirements and approve implementations based upon justification from the requesting Program Office
   - Implement the COMSEC Program in accordance with this Handbook and NSA Standards
   - Conduct internal audits, inventories and provide a copy of all findings to the NSI Program Team
   - Report all accounting irregularities, security violations or loss of COMSEC material immediately to the NSI Program Team
   - Select and designate, in writing, Primary and Alternate COMSEC Custodians (must be completed by the Federal Employee Program Manager)
   - Maintain documentation of all COMSEC equipment and materials within their area of responsibility for a minimum of five years

6. The COMSEC Custodian (Primary) shall:
   - Meet the following requirements and sign associated documentation:
     i. Be a U.S. Citizen (includes naturalized; immigrant aliens are not eligible)
     ii. Possess a final security clearance equal to, or higher than, the highest classification of COMSEC material to be held by the account
     iii. Be authorized, in writing, to access keying material by the COMSEC Controlling Authority

iv. Complete the COMSEC Access Briefing and NSA COMSEC Custodian training

- Be the subject matter expert on matters related to COMSEC and the COMSEC account administrative records, reports, and audits
- Maintain a working relationship with the NSI Program Team and the NSI Representatives responsible for NSI and COMSEC material, equipment or information management in their area of responsibility
- Maintain a list of authorized users, training records and User Agreements for a minimum of five years from the date of termination from the system
- Retain all COMSEC related documentation for a minimum of five years and provide a copy of all documentation to the NSI Representative
- Receive, issue, store and maintain all cryptographic keying material needed for the operation of EPA COMSEC equipment
- Utilize and maintain the COMSEC Material Control System (CMCS) inventory and management system
- Conduct reportable inventories for all COMSEC material
- Validate security clearances, need-to-know and issuing authorization prior to the issuing of any COMSEC equipment
- Verify semi-annually that all users/hand receipt holders are maintaining their COMSEC equipment
- Report all accounting irregularities, security violations or loss of COMSEC material immediately to the NSI Program Team
- Serve as the EPA OSWER Terminal Administrator for Secure Telephones
- Record and retain the user Personal Identification Numbers (PIN) and the Terminal Administrator (TA) PIN in an approved storage location commensurate with the classification level of the telephone issued
- Coordinate monthly testing and any required rekeying of COMSEC equipment with users and verify the condition and connectivity of each STE quarterly
- Provide training and equipment support to users

7. The COMSEC Custodian (Alternate) shall:
   - Meet all of the requirements as outlined for the Primary COMSEC Custodian
   - Assist the Primary COMSEC Custodian in the performance of their duties
   - Assume the duties of the Primary COMSEC Custodian in their absence
   - Share equally with the Primary COMSEC Custodian the responsibility for the proper daily management and administration of the COMSEC account

8. The National Security Information (NSI) Representative shall:
   - Assist the COMSEC Custodian with ensuring that users receive the proper training and authorizations for accessing COMSEC material
   - Assist the COMSEC Custodian, owners and users with all transactions and testing of COMSEC material or equipment quarterly at a minimum
   - Maintain a copy of documentation for all COMSEC equipment and materials within their area of responsibility

- Report all accounting irregularities, security violations or loss of COMSEC material immediately to the NSI Program Team and COMSEC Custodian

9. The Secure Terminal Equipment (STE) and Secure Cellular and Satellite Telephone (SCST) COMSEC Users (Hand Receipt Holder) shall:
   - Not relocate the STE telephone from an accredited space without the authorization of the COMSEC Custodian and NSI Program Team
   - Be an EPA federal or non-federal employee who is required to use a Secure Communication Device with COMSEC material in the performance of their official duties
   - Complete the following prior to being issued any COMSEC material:
     i. Complete EPA user training and sign an EPA User Agreement Form for their specific device as identified in Section 3
     ii. Sign a COMSEC Material Report Form also known as the "Hand Receipt" or the Standard Form 153 (SF-153) prior to accepting custody of COMSEC material
   - Be responsible for safeguarding COMSEC material
   - Provide all COMSEC material for review in a timely manner at the request of the NSI Representative, COMSEC Custodian, or NSI Program Team
   - Properly store the STE/Crypto Card and/or SCST/PIN and restrict access to them from unauthorized persons
   - Report all accounting irregularities, security violations or loss of COMSEC material immediately to the NSI Representative, COMSEC Custodian or NSI Program Team
   - Test the secure telephone quarterly in the secure mode
   - Refer to the STE and SCST SOPs for specific requirements and handling procedures
   - Semiannually or when requested by the COMSEC Custodian, physically sight the STE, Crypto Card and/or SCST and verify in writing to the Custodian the serial numbers of the equipment and Crypto Card
   - Ensure that only properly cleared and authorized persons have access to the STE or SCST when in the classified mode and all access requirements in Section 4 have been met
     i. Hand Receipt Holder must provide a list of individuals who will have access to and use the secure telephone and associated Crypto Card/PIN to the COMSEC Custodian and the NSI Program Team

10. All other COMSEC Users shall:
    This section does not apply to general users of Secure Terminal Equipment and Secure Cellular and Satellite Telephone. This section only pertains to other types of encrypted systems and equipment that utilizes COMSEC keying material (e.g. Secure Radio Communication systems, Secure Video Teleconferencing equipment)
    - Not relocate any COMSEC equipment from an accredited space without the authorization of the COMSEC Custodian and NSI Program Team

- Be an EPA federal or non-federal employee who is required to use a Secure Communication Device with COMSEC material in the performance of their official duties
- Complete the following prior to being issued any COMSEC material:
  i. Complete EPA user training and sign an EPA User Agreement Form for their specific device as identified in Section 3
  ii. Sign a SF-153 prior to accepting custody of COMSEC material
  iii. Complete the NSA/CSS Manual No. 3-16 COMSEC Access Briefing Form
- Be responsible for safeguarding COMSEC material
- Provide all COMSEC material for review in a timely manner at the request of the NSI Representative, COMSEC Custodian and NSI Program Team
- Properly store the COMSEC equipment and restrict access to it from unauthorized persons
- Report all accounting irregularities, security violations or loss of COMSEC material immediately to the NSI Representative, COMSEC Custodian or NSI Program Team

Section 3: Equipment

All COMSEC related devices shall be procured in coordination with the COMSEC Custodian and NSI Program Team. All COMSEC material will be provided by the EPA COMSEC Custodian. No other sources are permitted without prior authorization.

12-300 Controlled Cryptographic Item (CCI)

1. Controlled Cryptographic Item (CCI) equipment utilizes COMSEC encryption keying material to enable classified secure communications, generally referred to as "Keying Material, KeyMat, or Crypto Key". CCI equipment that is not keyed is unclassified unless otherwise marked; however it remains an accountable item that must be:
   - Controlled using COMSEC accountability procedures
   - Secured as a high dollar value item
   - Protected from tampering
   - Restricted from unauthorized access by uncleared personnel.

2. EPA employs a multitude of CCI equipment in a variety of configurations to properly secure and safeguard all communications
   - The user should refer to the specific SOP and manufactures instruction manual for further guidance

12-301 Secure Terminal Equipment (STE) and Crypto Card

1. The STE and associated Crypto Card will be issued by the COMSEC Custodian using an SF-153 after verification that the installation location has been accredited by the NSI Program Team in accordance with Chapter 5 and the Hand Receipt Holder has received the proper STE user briefings and signed the User Agreement Form.
   - Users are prohibited from transferring their issued COMSEC equipment or material to another user

- If more than one person will have access to the STE and Crypto Card, a full list of names will be provided to the COMSEC Custodian and the NSI Program Team; they will arrange STE user training and signing of the User Agreement Form for those individuals
- All equipment must be returned to the COMSEC Custodian for reissue
- The STE SOP contains the minimum security standards and guidance for the handling and management of the STE

12-302 Secure Cellular and Satellite Telephone (SCST)

1. The SCST will be issued by the COMSEC Custodian using an SF-153 after authorization has been received and the Hand Receipt Holder has received the proper SCST user briefings and signed the User Agreement Form.
   - Users are prohibited from transferring their issued COMSEC equipment or material to another user
   - If more than one person will have access to the SCST and PIN, a full list of names will be provided to the COMSEC Custodian and the NSI Program Team, they will arrange SCST user training and signing of the User Agreement Form for those individuals
   - All equipment must be returned to the COMSEC Custodian for reissue
   - The SCST SOP contains the minimum security standards and guidance for the handling and management of SCST equipment

12-303 Secure Video Teleconferencing System (SVTS)

1. The SVTS will only be installed in a space accredited by the NSI Program Team for amplified discussions up to the classification level of the system and used in accordance with the applicable security plan.
   - The SVTS SOP contains the minimum security standards and guidance for the operation, handling and management of SVTS equipment

Section 4: Access

The COMSEC user has the primary responsibility for all Personnel, Physical and Administrative Security requirements related to the safeguarding and accounting of COMSEC material and equipment in their possession or within their area of responsibility.

12-400 Requirements

1. Access requirements: Access to classified COMSEC material or information is limited to U.S. Citizens (by birth or naturalized) only, provided they have:
   - Completed the requirements of Chapter 5 Section 3
   - Been granted a final security clearance by the U.S. Government commensurate with the classification level of the COMSEC information
   - A valid need-to-know
   - Received the appropriate training, as identified in Chapter 7

2. Visitors: All uncleared visitors entering areas with COMSEC equipment must be escorted and kept under continuous observation by authorized personnel.

- Contractors or maintenance personnel requiring access to a secured area for major repairs or renovations must be approved in accordance with Chapter 5

12-401 Physical Security and Safeguarding COMSEC Material

The unique physical properties and retentive capabilities of magnetic media and COMSEC devices require special precautions be taken to safeguard all classified information stored on such media and in COMSEC devices. Safeguard any residual classified information that might reside within COMSEC media or equipment at the completion of classified processing. All users must follow the NSI Handbook and the specific SOP for safeguarding procedures for the COMSEC material or equipment they will be utilizing.

1. Secure Areas: Routine COMSEC operations shall only take place in a secure area that has been accredited in accordance with the standards established in Chapter 5, Section 6.

2. Storage Requirements: COMSEC users must comply with the following storage requirements for all issued COMSEC material, as referenced in Chapter 5, Section 6.
   - All removable classified COMSEC media, to include hard drives, floppy disks, CDs, etc. shall be stored in a GSA approved class 5 or 6 (letter or legal) security container, unless physically located within an accredited open storage area
   - If a classified computer system does not have a removable hard drive, the system itself shall be stored in a GSA approved security container unless physically located within an open storage area
   - All STE telephones and Crypto Cards must be stored and protected in a manner that is sufficient to preclude any reasonable chance of theft, sabotage, or tampering and in accordance with Chapter 5
     i. The STE and the Crypto Card(s) cannot be stored in the same room unless the Crypto Card is secured in a GSA approved security container
     ii. If stored in separate rooms a GSA security container is not required however the Crypto Card(s) must be secured (e.g. a locked drawer, locked container, lockbox or cabinet) to prevent access by unauthorized personnel
     iii. Access to the STE and Crypto Card must be restricted to only authorized users
   - All SCST and PINS must be stored and protected in a manner that is sufficient to preclude any reasonable chance of theft, sabotage, or tampering and in accordance with Chapter 5
     i. The SCST and the associated PIN cannot be stored in the same room unless the SCST and PIN are secured in a GSA approved security container
     ii. Access to the SCST and PIN must be restricted to only authorized users
   - The Security Container Information Form (SF-700) stored in a GSA approved security container is the only authorized method for annotating of any password, code or combination for access to classified information
     i. SCST PINs are unclassified unless associated with a secure telephone.

- Detailed methods for the management and handling of all COMSEC secure communication equipment are provided in the applicable SOPs

12-402 Administrative Security

1. User Agreement Forms: When signed, these forms are an acknowledgement, by the user, of their responsibilities to protect the communication device or system and all classified information received from or processed on this equipment.
   - EPA COMSEC User Agreement Form
   - STE User Agreement Form
   - SCST User Agreement Form

2. COMSEC Material Report Form 153 (SF 153): All CCI equipment and COMSEC material transactions will be conducted utilizing an SF-153, to record all movement, issuance, and transferring of all material to and from the COMSEC account.
   - COMSEC material or CCI equipment issued on an SF-153 will never be reissued, transferred or loaned by a user to another individual. All material and equipment must be returned to the COMSEC Custodian for reissue

3. COMSEC Operations Auditing: COMSEC auditing will be conducted by NSA Inspectors and the NSI Program Team on a periodic basis.

Section 5: Training

12-500 COMSEC Training Requirements

Mandatory COMSEC training is provided as a means to introduce authorized users to the proper use and protection of COMSEC equipment, COMSEC material and classified information.

1. STE and SCST User Training: All authorized STE and SCST COMSEC users shall complete the Initial NSI Orientation training prior to being issued COMSEC material. At a minimum, training will cover the operating procedures and protective measures established to protect classified information.
   - All users must complete the system specific Security Awareness training and must complete all training in Chapter 7, Section 3 and Section 5
   - Upon completion of training, a system specific COMSEC User Agreement Form must be signed by the user
   - Refresher training may be required
   - Users will be provided system specific equipment operational training as needed

2. All other COMSEC Users Training (Non-Telephone User):
   This section does not apply STE and SCST users, or general hand receipt holders.
   - In addition to the training identified in section 1, all COMSEC Custodians, Alternates and Managers must complete an NSA Annual COMSEC Refresher training as described in the NSA Policy Manual 3-16
   - Upon completion of training and refresher training, an EPA COMSEC User Agreement Form must be signed

- All COMSEC users or managers must complete a COMSEC in briefing and debriefing as described in NSA Policy Manual 3-16 Section II, paragraph 7

Section 6: Inspections

12-600 COMSEC Account Inspection, Inventory and Audit Requirements

1. Standard inspections, inventories and audits will be conducted by NSA.
   - NSA will conduct inspections and audits of the COMSEC account on a two year cycle and will establish the inspection dates, times, location and parameters
   - NSA will provide a reportable itemized inventory of the COMSEC account annually

2. Unannounced inventories, inspections and audits may be conducted by the NSI Program Team at the discretion of the SAO.
   - NSI Program Team will utilize NSA provided inspection checklist and inventory documentation, as needed

Section 7: Transmission

12-700 Transmission of COMSEC Material

All transmission or transfers of COMSEC material will be conducted in accordance with the procedures in Chapter 6 and NSA/CSS Policy Manual No. 3-16.

Section 8: Reportable Security Incidents

12-800 Reportable Security Incidents

All EPA personnel, federal and non-federal, are responsible for reporting any situation or incident related to the improper use, loss or compromise of COMSEC material. Listed below are some examples of the most common Reportable Security Incidents; however this list is not all inclusive. Any incident or circumstance, realized or suspected, that could potentially compromise classified information must be reported immediately to the proper authorities to prevent the loss of the information.

1. Practices Dangerous to Security: The following occurrences must be reported immediately (within 72 hours) to the NSI Program Team and the COMSEC Manager.
   - Receiving misdirected classified material that was not intended for the recipient
   - Transmission of classified information using COMSEC equipment that is suspected of being compromised
   - Suspected computer malicious code, viruses, trojan horses, computer worms or other software intended to cause interference or damage to the COMSEC equipment
   - Any observable abnormal occurrence while utilizing the COMSEC equipment
   - Suspected compromise or improper storage of any PIN, password, code, combination or Security Container Information Form (SF 700)
   - Use of the system for any purpose other than for official government business

2. COMSEC Incidents: The following examples are reportable COMSEC Incidents and must be reported immediately upon discovery to the NSI Program Team and the COMSEC Custodian.
   - Loss, theft or compromise of any COMSEC material or equipment
   - Known compromise, intentional and deliberate mishandling or improper storage of any password, Crypto Card, code, combination or Security Container Information Form (SF 700)
   - Any instances when a STE telephone and its Crypto Card are stored in the same room and not secured within a GSA approved container except in an accredited open storage area
   - Any instance where a Crypto Card is not properly stored within a limited access locked storage container
   - Any occurrence where an unauthorized person has access to the STE and Crypto Card
   - Known compromise, intentional and deliberate mishandling or improper storage of any SCST and its associated PIN
   - Any instance where an SCST PIN is affixed to the telephone or the PIN is associated to the SCST and is not properly secured
   - Any occurrence where an unauthorized person has access to the SCST and PIN. Any instance where the PIN is entered or stored with the SCST except in an accredited open storage area
   - Any evidence of possible tampering with, or unauthorized access to any secure telephone equipment, COMSEC equipment or COMSEC material
   - Unauthorized personnel observing or participating in classified operations
   - Intentional attempts to bypass, strain, test security mechanisms, violate security procedures, protocols or safeguards, or the connection of any non authorized ancillary device, software or medium on any COMSEC equipment or material without prior written authorization
   - Sharing or providing usage of passwords, PINs, combinations or codes to other personnel for access to any COMSEC equipment or material by someone other than the user it was issued to
   - Any instance where the display indicates that the distant terminal contains a compromised key
   - Any violation of the provisions outlined in this Chapter, or on any signed system User Agreement Form

Section 9: Emergency Action Plans

12-900 Emergency Action Plans

The COMSEC Custodian will establish, publish and properly display an Emergency Action Plan within the COMSEC storage facility to ensure the safe handling or destruction of all COMSEC material in the event of a man made or natural disaster, or other significant event.

The COMSEC Custodian will assist NSI Representatives and COMSEC users in the creation of Emergency Action Plans to properly safeguard COMSEC material in the event of a national disaster or national security threat.

Section 10: Destruction

12-1000 Destruction of COMSEC Material

The world wide usage of COMSEC material and the retentive capabilities of electronic devices require special precautions be taken to ensure the proper and timely destruction of COMSEC material. All destruction will be conducted in accordance with the NSI Handbook and the NSA/CSS Policy Manual No. 3-16.

1. Routine Destruction of COMSEC material: (Less Equipment)
   - All destruction of COMSEC material will be conducted by the Primary or Alternate COMSEC Custodian and witnessed by an appropriately cleared individual
   - General COMSEC users will not conduct destruction of COMSEC material without direct supervision and authorization from the COMSEC Custodian
   - All COMSEC material shall be properly accounted for and verified on an SF-153 by short title before, during and after the destruction process
   - All COMSEC Keying Material shall be destroyed within 12 hours of supersession unless otherwise authorized
     - Failure to complete the destruction within these time limits is a reportable COMSEC incident and the Controlling Authority must be notified immediately upon discovery of the incident
     - Premature destruction of COMSEC material will be reported to the Controlling Authority immediately and replacement material will be requested accordingly

2. Emergency Destruction of COMSEC material:
   - All emergency destructions will be in accordance with the COMSEC Emergency Action Plan

This page is intentionally blank

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.13526.

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 their 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, it 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. 13526, 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.

Cognizant Security Agency (CSA) - Agencies of the Executive Branch that have been authorized, by E.O. 12829, as amended 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.

Collateral Information – Information identified as National Security Information under the provisions of E.O. 13526, but not subject to enhanced security protection required for Special Access Program Information.

Communications Security (COMSEC) - The measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto-security, transmission security, emission security and physical security of COMSEC material.

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.

Controlled Cryptographic Item (CCI) - Identifies communication equipment critical to the COMSEC function of securing classified information and assumes the same classification as the information when in use. CCIs may be unclassified when not in use but are subject to special accounting controls and required markings.

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 publications. 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 instrumental 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. 13526.

DEFINITIONS

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. 13526 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.13526.

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.

DEFINITIONS

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. 13526 and its implementing directives.

Senior Agency Official - The official designated by the agency head under section 5.4(d) of E.O. 13526, 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.

This page is intentionally blank

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
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 DATA COLLECTION REPORT

Submission of this form is to be completed no later than October 15th of the current fiscal year to the NSI Program Team. To expedite the process of submission, please fax the form to 202-565-2028. ATTN: NSI Program Team

Part A: Identifying Information

1. Fiscal Year:

2. Area Location Information	3. NSI Representative Information
EPA Region:	Name:
Organization Name:	Work Phone:
Program Name:	Fax Number:

Part B: Original Classification Decisions

Original classification is an initial determination that the information to be classified 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 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. 13526 and; (4) disclosure could reasonably be expected to result in damage to the national security. [Provide information on all classification decisio ns, regardless of media, including those documented and disseminated via e-mail. 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.**
2. 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 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.**

Part 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. [Provide information on all classification decisions, regardless of the media, including those documented and disseminated via e-mail. Do not count reproductions or copies. 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.**
2. Enter the number of **derivative CONFIDENTIAL** classifications during the reporting period.	**3.**
4. Total number of derivative classifications decisions. (Sum of blocks 1, 2 and 3)	**4.**

Appendix D SELF-INSPECTION CHECKLIST

This page is intentionally blank

SELF-INSPECTION CHECKLIST

NSI Management

Yes	No	N/A	
☐	☐	☐	1. Does the NSI Representative maintain up-to-date copies of appropriate orders, directives, manuals, handbooks and guides?
☐	☐	☐	2. Does the NSI Representative develop and maintain local SOPs for his/her NSI related activities?
☐	☐	☐	3. Are local SOPs part of the security orientation for assigned personnel with clearances?
☐	☐	☐	4. Do producers and users of classified information receive guidance with respect to security responsibilities and requirements?

Security Incidents and Reporting Requirements

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

Classification Management

☐	☐	☐	11. Does the NSI Representative have a method to track all original and derivative classification decisions in his/her area of responsibility?
☐	☐	☐	12. Do subject matter experts that develop information requiring an original classification decision understand the process to obtain a decision from the OCA?
☐	☐	☐	13. Are documents pending an original classification decision safeguarded in a manner prescribed according to its proposed classification?
☐	☐	☐	14. Do local procedures prohibit the use of terms such as “FOUO” or “Secret Sensitive” for the identification of classified NSI?
☐	☐	☐	15. If classification challenges occur, have the proper procedures been followed?
☐	☐	☐	16. 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

☐	☐	☐	17. Are classified documents properly marked to include all applicable markings (e.g., overall, page, and portion markings)?
☐	☐	☐	18. Are originally classified documents marked with a classification block that consists of "Classified by", "Reason", and "Declass on" lines?
☐	☐	☐	19. Are derivatively classified documents marked with a classification block that consists of “Classified by”, "Derived from" and "Declass on" lines?

Yes	No	N/A	
☐	☐	☐	20. Does the derivative classifier maintain a copy of the original source document with the derivatively classified document?
☐	☐	☐	21. Are markings on derivative classified documents consistent with the classification markings on the source information?
☐	☐	☐	22. Is classified information such as maps, charts, graphs, photographs, slides, recordings, videotapes, and computer media appropriately marked?
☐	☐	☐	23. Are working papers dated when created, marked "Working Paper", and brought under accountability after 180 days or when they are released outside the Agency?
			Safeguarding
☐	☐	☐	24. 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?
☐	☐	☐	25. Are procedures in place for classified meetings to be held within the facility?
☐	☐	☐	26. Does the NSI Representative, maintaining 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?
☐	☐	☐	27. Do all cleared employees who resign, transfer, or retire return all classified information in their possession?
☐	☐	☐	28. Are procedures established for end-of-day security checks, to include use of the SF 701 and SF 702?
☐	☐	☐	29. Are classified cover sheets (e.g., SF 703, SF 704, and SF 705) placed on all classified information when removed from secure storage?
☐	☐	☐	30. Are media marking labels (e.g., SF 706, SF 707, SF 708, and SF 712) being utilized on all classified computer media?
☐	☐	☐	31. Are there dedicated copy machines with signs posted on the machine to indicate the level of classified that may or may not be reproduced?
☐	☐	☐	32. Is all classified information including copies, originated or received by the program or facility, continuously accounted for, individually serialized, and entered into Drawer Inventory logs?
☐	☐	☐	33. Is all classified information accounted for at least annually, at the change of NSI Representatives, and upon report of loss or compromise of information or information?
			Storage
☐	☐	☐	34. Is classified information stored under conditions that will provide adequate protection and prevent access by unauthorized personnel?

SELF-INSPECTION CHECKLIST

Yes	No	N/A	
☐	☐	☐	35. Does the NSI Representative ensure that external markings on security containers do not reveal the level of information stored within?
			36. Are container combinations changed:
☐	☐	☐	• By individuals who possess the appropriate clearance level and need-to-know?
☐	☐	☐	• 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 has been put into or taken out of service?
☐	☐	☐	37. Are SF 700s utilized to maintain security container information?
☐	☐	☐	38. Are SF 700s properly marked to indicate the level of classification of the combination, with Attachment 1 affixed to the inside of each security container?
☐	☐	☐	39. Does the SF 700 include the names, home addresses, and phone numbers of all persons having knowledge of the combination?
☐	☐	☐	40. Does the NSI Representative maintain a copy of all accreditations?
☐	☐	☐	41. Does the NSI Representative utilize the Accreditation Status Form and Classified Equipment Form to communicate accreditation status with the NSI Program Team?
			Destruction
☐	☐	☐	42. Are reviews conducted periodically to ensure classified information is destroyed when no longer required?
☐	☐	☐	43. Are all classified information shredders NSA-approved crosscut shredders?
☐	☐	☐	44. Are records of Top Secret destruction maintained in the Drawer Inventory accountability files?
			Transmission Methods
☐	☐	☐	45. Are classified information receipts used for transferring documents between facilities or agencies?
☐	☐	☐	46. Are receipts for Top Secret information retained for 5 years and receipts for Secret information retained for 2 years?
☐	☐	☐	47. Does the NSI Representative ensure that only authorized and appropriately cleared personnel transmit, transport, escort, or hand-carry classified information?
☐	☐	☐	48. Has the NSI Representative developed local procedures to ensure classified information can be tracked, properly disseminated, and quickly detected if lost?

SELF-INSPECTION CHECKLIST

Yes	No	N/A	
☐	☐	☐	49. Has the NSI Representative developed and implemented local procedures to protect incoming mail, bulk shipments, and items delivered by messenger containing classified information?
☐	☐	☐	50. Are secure phones installed in appropriately accredited areas?

Education and Training

☐	☐	☐	51. Have all cleared personnel received initial security orientation training?
☐	☐	☐	52. Is there a continuing security awareness program that provides for frequent exposure of cleared personnel to security awareness information?
☐	☐	☐	53. Are termination briefings given to employees who leave the organization or whose clearance is terminated?

Industrial Security Program

☐	☐	☐	54. Does the CO issue and sign all DD 254s?
☐	☐	☐	55. Does the COR validate all contractor personal security clearances?
☐	☐	☐	56. Does the COR and NSI Representative verify FCLs and storage capability prior to release of classified information?
☐	☐	☐	57. Do the issued DD 254s provide additional security requirements?
☐	☐	☐	58. Does the COR verify that cleared contractor employees who are used as couriers have been briefed on their courier responsibilities?

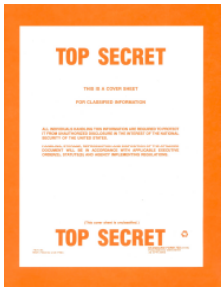
Notes:

This form is to be submitted to the NSI Program Team no later than October 15 of the current fiscal year. To expedite the process of submission, please fax the form to: 202-565-2028 or email to ProgramTeam.NSI@epa.gov ATTN: NSI Program Team	
Date:	
NSI Representative Name: Program Office or Region: Program Name:	

Appendix E SAMPLES OF STANDARD FORMS

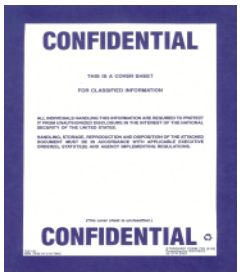
This page is intentionally blank

SAMPLES OF STANDARD FORMS



SF 703
Top Secret Cover Sheet
(Orange/White)

SF 704
Secret Cover Sheet
(Red/White)



SF 705
Confidential Cover Sheet
(Blue/White)

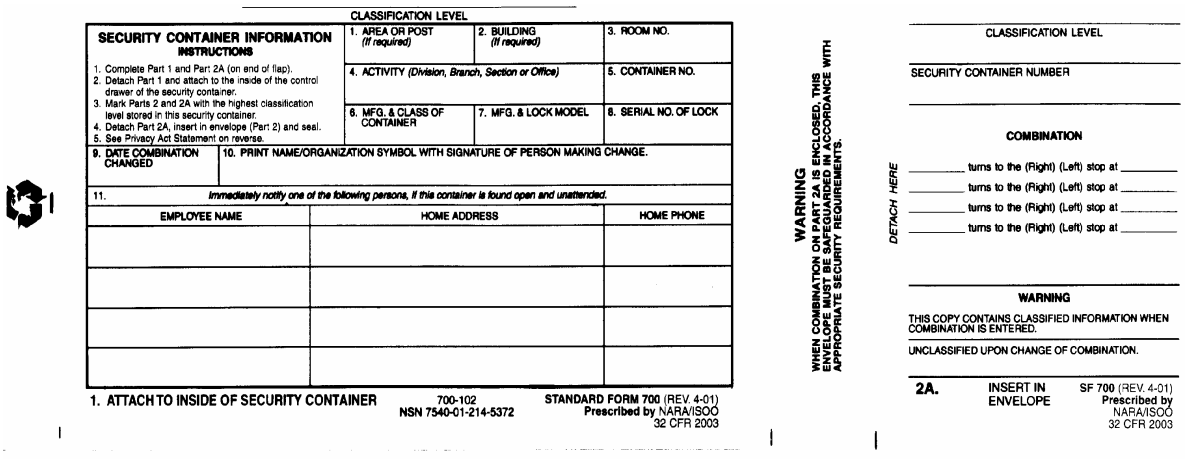
SF 706
Top Secret Label
(Orange)

SF 707
Secret Label
(Red)

SF 708
Confidential Label
(Blue)

SF 710
Unclassified Label
(Green)

Sample SF 700 (Security Container Information Form)



CLASSIFICATION LEVEL

SECURITY CONTAINER INFORMATION
INSTRUCTIONS

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 this security container.
4. Detach Part 2A, insert in envelope (Part 2) and seal.
5. See Privacy Act Statement on reverse.

1. AREA OR POST *(If required)*	2. BUILDING *(If required)*	3. ROOM NO.
4. ACTIVITY *(Division, Branch, Section or Office)*		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. *Immediately notify one of the following persons, if this container is found open and unattended.*

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF SECURITY CONTAINER

700-102
NSN 7540-01-214-5372

STANDARD FORM 700 (REV. 4-01)
Prescribed by NARA/ISOO
32 CFR 2003

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED 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 _____

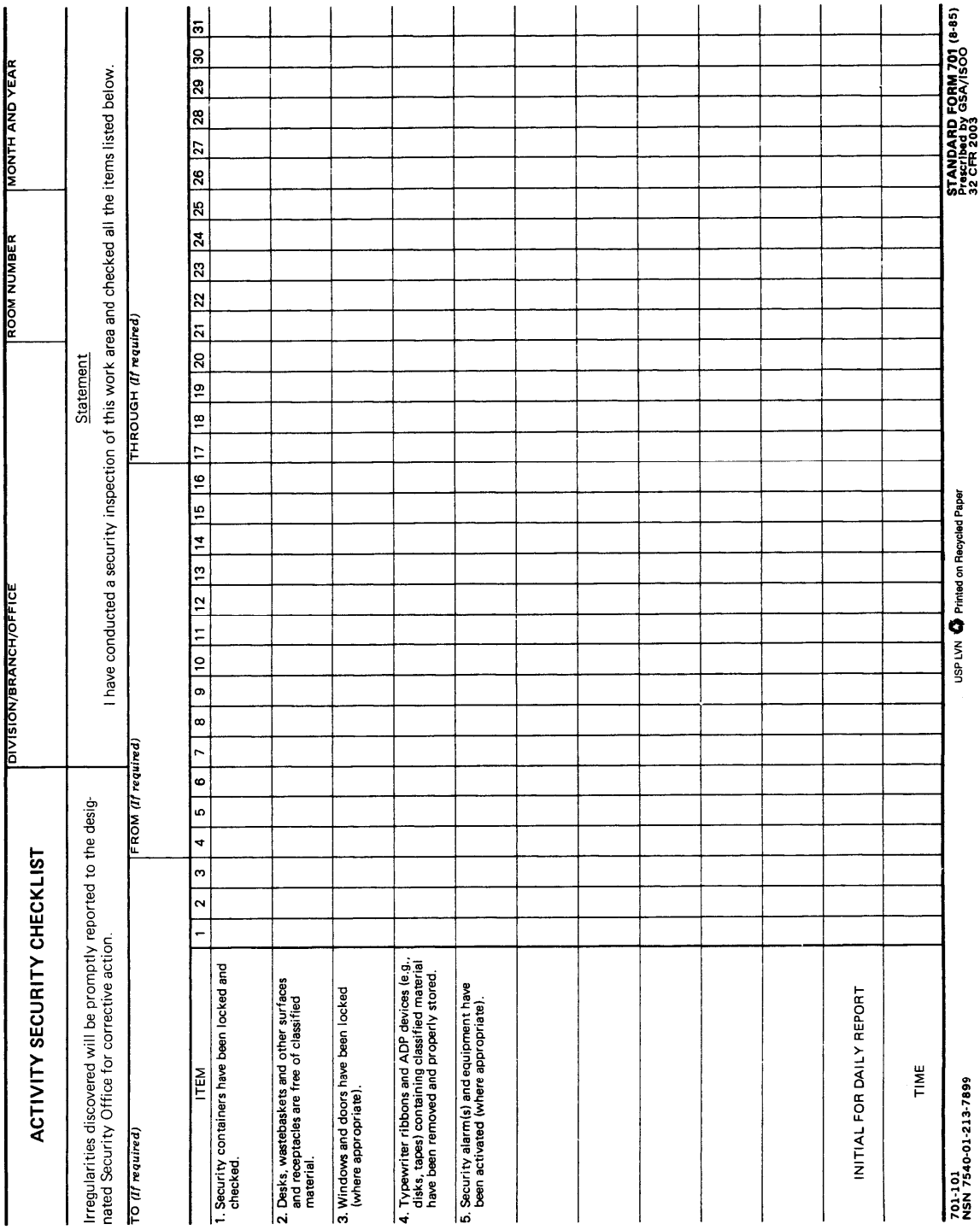
WARNING

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



ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE | ROOM NUMBER | MONTH AND YEAR

Statement

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
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/ISOO
32 CFR 2003

Sample SF 701 (Activity Security Checklist)

SECURITY CONTAINER CHECK SHEET

TO (if required)	THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISOO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

Sample SF 702 (Security Container Check Sheet)

Appendix F ROOM ACCREDITATION CHECKLIST

This page is intentionally blank

ROOM ACCREDITATION CHECKLIST

Section A
Secure Area Information

1. Type of Accreditation Request: (select one)

☐ New Accreditation

☐ Change Accreditation Level
(e.g. from Secret to Top Secret)

2. Level of Classified Information in the Room (mark all that apply)

☐ Top Secret

☐ Secret

☐ Confidential

3. Room will be used for:
(mark all that apply)

☐ Classified Information Review
☐ Classified Discussions
☐ Classified Processing
☐ Classified Storage
☐ Classified Destruction

4. Indicate Type of Area:
(select one)
☐ Continuous Handling
(24 hr Open Storage)
☐ 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?

☐ Yes (complete block 9)
☐ No

9. Prior Accreditation Information: (if applicable)

Accreditation Number:

Accreditation Granted By:

Accreditation Date:

Section B
Room Access Control Feature(s)

1. Is there a system in use that controls entry and visitor access to the room?

☐ Yes (complete block 2)

☐ No

2. Describe the type of entry and access control(s).

☐ Card Reader
☐ Passes or ID Badges
☐ Access List
☐ Visitor Escort
☐ Other:

Section C
Room Construction Features

1. Walls, Ceilings, and Floors

a. Do the perimeter walls extend from true floor to true ceiling?
☐ Yes (complete block 2)
☐ No

b. Are the perimeter walls permanently constructed?
☐ Yes (complete block 2)
☐ No

c. Are the perimeter walls attached to each other? (i.e. **NOT** cubicles)
☐ Yes (complete block 2)
☐ No

d. Is the ceiling a false ceiling? **(open storage only)**
☐ Yes (complete block 3)
☐ No

e. Is the floor a false floor? **(open storage only)**
☐ Yes (complete block 4)
☐ No

f. Do vent ducts penetrate the walls **(open storage only)**
☐ Yes (complete 5)
☐ No

2. Describe material and thickness of the room's perimeter walls, ceiling, and floors.

3. What is the distance between the false ceiling and the true ceiling?

4. What is the distance between the false floor and the true floor?

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).

Room Construction Features (continued)

6. Doors

a. Type of door(s). (complete block 7)
☐ Wood
☐ Metal

b. Do/does the door(s) have a solid core?
☐ Yes
☐ No

c. Location of door hinges.
☐ Interior to the space
☐ Exterior to the space (complete block 8 if in an uncontrolled area)

d. Type of lock on door.
☐ Electronic (X07, X08, X09) (complete block 9)
☐ Cypher (complete block 9)
☐ Keyed
☐ None

7. Describe the room entrance and exit door(s).
(e.g. number, thickness, windows, automatic door closer, deadbolts, panic hardware)

8. Describe how the door hinges exterior to the room are secured against removal. (e.g. welded)

9. Where is the door lock combination stored?

10. Windows

a. Does the space have windows?
☐ Yes
☐ No (proceed to section D)

b. How are windows protected against visual surveillance?
☐ Opaque glass
☐ Drapes/Curtains
☐ Blinds
☐ Other (complete block 11)

c. Are windows at the ground level?
☐ Yes (complete block 12)
☐ No

d. Are ground windows monitored with an IDS?
☐ Yes
☐ No
☐ Not Applicable

11. Describe window covering.

12. If windows are at ground level, describe how they are secured against opening. (e.g. permanent seal, locking mechanism)

Section D
Room Sound Attenuation

1. With all doors closed, check which best describes the sound barrier performance of walls, ceilings, floors, windows, and doors.

☐ Normal speech can be heard and understood
☐ Normal speech can be heard but not understood
☐ Loud speech can be understood fairly well. Normal speech cannot be easily understood.
☐ Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly if at all.
☐ Loud speech can be faintly heard but not understood. Normal speech is unintelligible.
☐ 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.

2. Does the space utilize sound cover or masking? (Complete Block 3)

☐ Yes
☐ No

3. Describe the type of sound cover or masking utilized. (e.g. white/pink noise, wall mounted transducer, cd player, television, etc.)

Section E
Classified Equipment in Room

1. Describe the type of secure phone issued. (if applicable)

☐ STE

Classification level of encryption key:
☐ Secret ☐ Top Secret

Make/Model:
Secure Phone #:

2. Describe the type of secure facsimile: (if applicable)

Make:
Model:

3. Describe the type of NSA approved shredder: (if applicable)

Make:
Model:

4. Is there a classified computer used in the room?

☐ Yes ☐ No

5. Classification level of computer:

☐ Confidential ☐ Secret ☐ Top Secret

6. Describe the type of classified computer used in the room: (e.g. laptop, desktop)

7. SSAA registration number:

Section F
Storage Container in Room

1. Will classified be stored in this space?

☐ Yes (complete block 3)
☐ No

2. Level of classified storage required?

☐ Top Secret ☐ Secret ☐ Confidential

3. Type of container utilized?

☐ GSA approved class 5 or 6 safe
☐ Legal size ☐ Letter size ☐ Other:

Container Make and Serial Number(s):

ROOM ACCREDITATION CHECKLIST

Section G **Supplemental Controls**	
1. Choose one of the supplemental controls that is being utilized: (open storage area and secure area with TS storage only) ☐ The location that houses the open storage area is under continuous (24 hr) protection by cleared guard or duty personnel; (complete block 2) ☐ 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) ☐ 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) ☐ Security-In-Depth conditions provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740	**2. Clearance level of guards:** ☐ None ☐ Top Secret ☐ Secret ☐ Confidential **3. Define the type of IDS utilized.** ☐ Motion Detection ☐ Alarms ☐ Other: _____ Note: Provide IDS specification with submission of this form. **4. Where is the IDS monitored?**

Section H **Additional Required Information**
1. Provide one of the following: ☐ Floor plan sketch of the area for accreditation (showing dimensions) and the immediate surrounding area/offices. ☐ Design Intent Drawings (if building out the area from scratch)

Section I **Signature Block**		
1. Requester Name:	**2. Date:**	**3. Requester Signature:**
4. NSI Representative or NSI Program Team Member Name:	**5. Date:**	**6. Signature:** I have verified that all the information above is correct**.**

This page is intentionally blank

Appendix G ACCREDITATION STATUS FORM

This page is intentionally blank

ACCREDITATION STATUS FORM

Secure Area Information

Type of Accredited Room:	**Level of Accreditation:**	**Region, Facility Name, Address:**	**Responsible NSI Representative:**
☐ Open Storage Area ☐ Secure Area	☐ TS ☐ S ☐ C		Name: Phone: Email:
Accreditation Number:		**Accreditation Official:**	**Accreditation Date:**

Section A - Accreditation Status/Request

To be completed by the NSI Representative

☐ **Accreditation Suspended** ☐ **Request Recertification** ☐ **Request Withdrawal** ☐ **Change Operations** ☐ Review ☐ Discussion ☐ Processing ☐ Storage ☐ Destruction	**Action or Reason:** My signature confirms that I have verified the continued accuracy of the Secure Room Accreditation Checklist.	
NSI Representative:	**Date:**	**Signature:**

Section B - Accreditation Recertification

To be completed by the NSI Program Team

☐ **Action Required** ☐ **Approved** ☐ **Disapproved**	**Action or Reason:**	
Accreditation Official Name:	**Date:**	**Signature:**

Section C - Accreditation Withdrawal

To be completed by the NSI Program Team

☐ **Approved** ☐ **Disapproved**	**Reason:**	
Accreditation Official Name:	**Date:**	**Signature:**

Revised (06-09)

This page is intentionally blank

Appendix H CLASSIFIED INFORMATION ACCOUNTABILITY RECORD

This page is intentionally blank

CLASSIFIED INFORMATION ACCOUNTABILITY RECORD

United States Environmental Protection Agency
Washington, DC 20460

EPA Control Number

Classified Information Accountability Record

Section I. General

To:	From:

Date Transferred	Package Tracking Number

Section II. Description

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

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

☐ Receipt of information acknowledged	☐ 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 (All SCI and 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 Number	Copy Number	Date	Printed Name of Witnessing Official	Signature

EPA Form 1350-2 Revised 6/2010

This page is intentionally blank

Appendix I COURIER DOCUMENTATION

This page is intentionally blank

COURIER DOCUMENTATION

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 #*

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)	☐	---
2. Packaged and Sealed Material	☐	---
3. Completed the Classified Information Accountability Record	☐	---
4. Received a signed "Authorization to Transport Classified Government Information aboard a Commercial Aircraft" Memorandum, when required	☐	☐
5. Obtained Maps, if driving	☐	☐
6. *Debriefed After Trip	☐	---

***** 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.

COURIER DOCUMENTATION

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 their 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.

COURIER DOCUMENTATION

(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 their 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 their 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 SCI AUTHORIZATION REQUEST FORM

This page is intentionally blank

SCI AUTHORIZATION REQUEST FORM

United States Environmental Protection Agency
Washington, DC 20460

SCI Access 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 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
1200 Pennsylvania Ave, NW
Mail Code: 3206R
Washington, D.C. 20460

This page is intentionally blank

Appendix K SCI VISIT CERTIFICATION REQUEST FORM

This page is intentionally blank

SCI VISIT CERTIFICATION REQUEST FORM

United States Environmental Protection Agency Washington, DC 20460 **SCI Visit Certification Request Form**	**Date:**

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

Appendix L CLASSIFIED EQUIPMENT FORM

This page is intentionally blank

CLASSIFIED EQUIPMENT FORM					
Region or Program Office:				Date Verified:	
NSI Representative:				Signature:	
Address:			Room Number: Occupant:	☐ Add Equipment ☐ Remove Equipment ☐ Recertification	
Authorized Accreditation Level	C: ☐	S: ☐	TS: ☐	SCI:☐	Accreditation Number:

Type	**Classification Level Authorized**	**Make/Model**	**Notes**
Secure Telephone			
Secure Facsimile			
Security Container			
Shredder			
Computer			

Revised (06-09)

This page is intentionally blank

Appendix M CLASSIFIED INFORMATION CHAIN OF CUSTODY RECORD

This page is intentionally blank

CLASSIFIED INFO CHAIN OF CUSTODY RECORD

United States Environmental Protection Agency
Washington, DC 20460

Date

Classified Information Chain of Custody Record

Section I. General

To:	From:

Section II. Description

EPA Control Number	Package Description (unclassified whenever possible)

Section III. Receipt / Chain of Custody

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

EPA Form 1350-5 (06-07)

This page is intentionally blank

APPENDIX N PHYSICAL SECURITY ROOM SPECIFICATIONS

This page is intentionally blank

Revised: March 28, 2011

PHYSICAL SECURITY ROOM SPECIFICATIONS

Accreditation Requirements: Discussions need to take place prior to determine what will be required for accreditation. To assist with the accreditation process, the NSI Representative and the NSI Program Team needs to be involved in the review process of the drawings. Request you submit modified drawings when changes are made. During the build out, request you take photographs of the build out.

ENTRANCE DOOR

- The entrance doors must be 1 ¾-inch solid core wood door, or of equivalent quality.
- Door, frame and any applied sound attenuation material in seams must meet Sound Transmission Class (STC) rating of 50
- The door must be plumbed in its frame and equipped with the following:
    - A Lockmasters LKM7000 lock with an X-09 combination lock attached
    - A two factor card reader/pin pad is also required
    - A Balanced Magnetic Switch (BMS) door contact with enclosed steel wire chase.
    - A heavy duty automatic door closer must be installed on the interior of the door
    - A door sweep must be installed on the interior. Another acceptable type of door sweep is a drop door sweep.
    - Hinges are to be on the interior of door. If door is equipped with hinge pins located on the exterior side of the door where it opens into an uncontrolled area outside the facility, the hinges will be treated to prevent removal of the door (e.g. welded, set screws, etc.).
- The door frame must be filled with sound attenuating material and secured in place for both stability and sound attenuation purposes.
    - Door frames are recommended to be grout filled, even at stud walls, and the lockset or electric strike should include a strike "mortar guard" that is installed on the back side of the frame to prevent grout spilling out the strike opening. In addition, jamb supporting studs are recommended to be doubled and horizontally braced with 16-gauge metal plates or metal studs, to adjacent studs to prevent "pry-open" opportunities. Grout fill of the frames also improves sound isolation. Grout fill may require a special consideration to field drill a 3/4-inch hole at the top of the jamb to allow grout injection, followed by a cap secured over the hole. This requirement should be coordinated with the frame manufacturer.
    - Approved sound seal and/or weather stripping must be placed on the door frame where the door meets the frame. This needs to be installed on the interior of the door frame to prevent tampering.

WALLS

- All perimeter walls must be permanently affixed to the raised floor and extend to true ceiling (slab) and be constructed in a manner that meets a minimum Sound Transmission Code of 50 (STC50)

- For walls of drywall/stud construction:
    - Walls must be constructed of 3 5/8 inch metal studs, maximum 24 inches on center true floor to true ceiling (slab to slab)
    - Exterior wall to be composed of minimum one (1) layer of 5/8 dry wall; stagger seams from layer to layer, tape and mud all seams
    - Interior wall to be composed of minimum two (2) layers of 5/8 inch dry wall or such number of layers required to meet STC 50; staggered seams, tape and mud all seams
    - On interior wall over final layer of drywall install one (1) layer of sound absorbing material, specification sheets for recommended material to be provided by D/A to EPA Security Management Division for review prior to purchase and installation.
    - All existing conduit junction boxes/power receptacles not being abandoned/removed should have appropriate box extensions installed to accommodate the additional thickness of the walls.
        - All abandoned conduit to be removed or permanently capped at both ends.
    - The spaces between the studs must be filled with sound deadening material. The material must be attached in such a manner to prevent the insulation from sliding down and leaving a void at the top
- All penetrations of drywall, including above any false ceiling, must have all holes patched and cracks/seams finished with tape and mud
- All structural surfaces above the false ceiling must be painted for a finished look to reveal any attempts at penetration. Exterior walls should be painted above any false ceiling for same reason.

SOUND ATTENUATION

- White noise system and door transducer installed helps sound issues.
- One (1) sound masking white noise unit with integrated volume control installed in the room with speakers installed inside of the walls and ceiling facing out ward to prevent anyone from hearing the conversations outside of the room. Also, a door transducer must be installed on the door. Specification sheets for recommended material to be provided to EPA Security Management Division for review prior to purchase and installation

CEILING - Ducts, Vents, and other openings

- Duct work may need non conducting sleeves at each end or a sound system installed within it, usually pink noise.

- All vents, ducts, pipes and similar metallic penetrations to the room perimeter should have a non-conductive break on the interior perimeter of the room, as close to the wall as possible. This may not be possible for sprinkler systems due to local fire/safety code requirements. For existing vents, ducts and pipes, grounding at the point of entry and exit and wrapping with acoustic material can be used instead of retrofitting with a dielectric break.

- All vents, ducts and similar openings in excess of 96 square inches that enter or pass through the room must be protected with either man bars or grills
    - Man bars must be ½ inch diameter steel bars welded on center every six inches horizontally and vertically and secured from inside the area
    - Grills must be of 9-gauge expanded steel
- Any open air returns 96 square inches or more must have the same man bar assembly and inspection ports and in addition have a double 90 degree sound baffle (NOTE: this will cause a restriction to HVAC air flow)
- Inspection ports must be
    - Within the room and lockable
        - If the inspection port must be installed outside of the room, it must be padlocked.
    - Large enough and in a location to allow easy visual inspection of the man bar assembly
    - Must be closed and locked to prevent access after construction has begun.
- All ductwork, conduit, and pipes passing through the room should be treated for sound. This can be accomplished by inserting non-conductive breaks/material and/or sound/vibration dampeners on the interior side of the perimeter areas of the room where ductwork, conduit, and pipes penetrate the room. Additionally, ductwork should be interior lined or wrapped for sound attenuation purposes.
    - One (1) sound masking white noise device shall be attached to each duct, vent or pipe that penetrates the perimeter wall of the secure room.
- All holes around any pipe/vent or duct entering the perimeter of the room must be sealed with fire rated mud, foam, chalk etc.
- All pipes/conduits not being used must be removed, capped off or filled.

FLOOR

- Carpet shall be installed on the floor

WINDOWS

- All windows which might reasonably afford visual observation of classified activities shall be opaque or equipped with blinds, drapes or other coverings.

- Windows at ground level will be constructed from or covered with materials which provide protection from forced entry. The protection should be no stronger than the strength of the contiguous walls.

INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system must be installed inside the room with personnel responding within 15 minutes for Top Secret material or Open Storage.

An intrusion detection system will consist of:

- Installation of a minimum of one (1) motion detection sensor (passive, ultrasonic etc) within each room is required, positioned to detect the slightest opening of the entrance door. Depending on size of room and coverage additional motion detectors may be required.

- Balance Magnetic Switch (BMS) must be installed on the entry door

- An alarm keypad must be installed in the room that allows the employee to enter a number to activate and deactivate the IDS.

- IDS is to be independent from other systems safeguarding other protected areas.

- If an Access Control System (ACS) and IDS are integrated, they must operate independently. The ACS shall be subordinate in priority to reports from the IDS.

- IDS transmission lines leaving the SCIF and SAF must be encrypted at 128-bit (or greater).

- IDS back-up power can be from battery, generator, or both. However, if battery is the sole source of backup power, it must provide a minimum of 24 hours (UL-1076) of back-up power.

- IDS must provide visual and audible indication at both the monitoring station and keypad within the room of alarm activation, equipment tampering, equipment failure, transmission loss, loss of AC and DC power, and switching between AC and DC power.

- Accessing or securing the IDS must be accomplished from inside the room having its own arming/disarming station installed inside by the entry door.
    - IDS must have unique ID/passwords for individuals to access/secure the system.
    - IDS control unit, keypad, sensors, and wiring connecting these items shall be located within the SCIF
    - Premise Control Unit (PCU), some alarm companies call it a Remote Terminal Unit (RTU) or Control Panel must be wall mounted within the SAF. This is what receives the signals from all the associated sensors in the room and sends the alarm status to the Monitoring Station. This panel shall be equipped with tamper switches that are activated whenever the cover is removed or the panel is removed from its installation location
- All junction boxes serving the IDS and ACS of a secure room shall be located within that secure room.

SECURITY CONTAINERS

- All National Security Information (Top Secret, Secret, and Confidential) must be stored in a GSA approved Class 5 or 6 security container equipped with an X09 combination lock.

DESTRUCTION

- NSA approved shredder is required for destruction of classified material.

This page is intentionally blank

APPENDIX O Drawer Inventory Log

This page is intentionally blank

United States Environmental Protection Agency
Washington, DC 20460

Drawer Inventory Log

Container Number

Office/Room Number

Control Number / Date of Receipt	**Copy Number / Date of Material**	**Media Type**	**Item Description (unclassified title, # of pages, originator)**	**Point of Contact**	**Destroyed / Transferred**
Control Number:	Copy Number:	☐ Paper ☐ Diskette ☐ CD ☐ Hard Drive ☐ Other		Name:	☐ Destroyed ☐ Transferred
Date of Receipt:	Date of Material:		Class Level: ☐ TS ☐ S ☐ C ☐ SCI	Phone:	Date:
Control Number:	Copy Number:	☐ Paper ☐ Diskette ☐ CD ☐ Hard Drive ☐ Other		Name:	☐ Destroyed ☐ Transferred
Date of Receipt:	Date of Material:		Class Level: ☐ TS ☐ S ☐ C ☐ SCI	Phone:	Date:
Control Number:	Copy Number:	☐ Paper ☐ Diskette ☐ CD ☐ Hard Drive ☐ Other		Name:	☐ Destroyed ☐ Transferred
Date of Receipt:	Date of Material:		Class Level: ☐ TS ☐ S ☐ C ☐ SCI	Phone:	Date:
Control Number:	Copy Number:	☐ Paper ☐ Diskette ☐ CD ☐ Hard Drive ☐ Other		Name:	☐ Destroyed ☐ Transferred
Date of Receipt:	Date of Material:		Class Level: ☐ TS ☐ S ☐ C ☐ SCI	Phone:	Date:
Control Number:	Copy Number:	☐ Paper ☐ Diskette ☐ CD ☐ Hard Drive ☐ Other		Name:	☐ Destroyed ☐ Transferred
Date of Receipt:	Date of Material:		Class Level: ☐ TS ☐ S ☐ C ☐ SCI	Phone:	Date:
Control Number:	Copy Number:	☐ Paper ☐ Diskette ☐ CD ☐ Hard Drive ☐ Other		Name:	☐ Destroyed ☐ Transferred
Date of Receipt:	Date of Material:		Class Level: ☐ TS ☐ S ☐ C ☐ SCI	Phone:	Date:

This page is intentionally blank

January 2012

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/oaintran/smd/nationalsec.htm