U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 12.1	NRC FACILITY SECURITY PROGRAM	DT-16-39
Volume 12:	Security	
Approved By:	Victor M. McCree Executive Director for Operations	
Date Approved:	September 28, 2016	
Expiration Date:	September 28, 2021	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Denis Brady 301-415-5768	

EXECUTIVE SUMMARY

Management Directive (MD) 12.1, "NRC Facility Security Program," is revised to incorporate new requirements of—

- Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."
- Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (FIPS PUB 201-2).
- The latest Interagency Security Committee (ISC) Standards.
- Other U.S. Nuclear Regulatory Commission policy changes related to physical security requirements.

This MD has been revised to facilitate ease of reference and for clarity. As a result, information from several sections (e.g., prior MD 12.1 section entitled "Facility Clearance and Surveys") have either been modified, removed, or reorganized. This revision reflects updates to sections regarding the Industrial Security Program; Security Incident Program; visitor procedures; Personal Identity Verification (PIV) cards; temporary visitor, employee, and contractor badges; Occupant Emergency Plan (OEP); security container management; security assessments and surveys; key and lock program; and controlled, administratively controlled, limited access, and security controlled areas. In addition, this revision incorporates the courier card process, onsite and offsite public meeting and hearing security support process, the REAL ID Act, Insider Threat Program (ITP), Protective Threat Assessment Team (PTAT), foreign and domestic travel threat response process, and Criminal History Program (CHP).

EXECUTIVE SUMMARY

This revision also incorporates recommended changes resulting from the Office of the Inspector General (OIG) Audit 16-A-10 regarding the standards for offices to appoint room owners (i.e., Access Reviewing Officials (ARO)) and notify the Office of Administration (ADM) of changes to access rights for limited access areas, and OIG Audit 12-A-12 regarding the restructured reporting process for safeguards information.

TABLE OF CONTENTS

I. POLICY

It is the policy of the U.S. Nuclear Regulatory Commission to provide physical security requirements and procedures to protect personnel, classified information, sensitive unclassified information, facilities, and NRC assets. This management directive (MD) does not affect Commission rules and regulations applicable to NRC licensees that are contained in the *Code of Federal Regulations* (CFR).

II. OBJECTIVES

- Ensure that NRC facilities and personnel are protected from damage and harm to the greatest extent possible.
- Ensure that classified and sensitive unclassified information is protected from unauthorized access or disclosure consistent with pertinent laws, Executive Orders, MDs, and applicable directives of other Federal agencies and organizations.
- Promote NRC security awareness and manage the NRC Security Incident Program.
- Ensure the limitation on wiretapping and eavesdropping devices in NRC facilities.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Executive Director for Operations (EDO)

Provides oversight for agencywide policies and goals relative to the NRC Facility Security Program.

B. Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital Programs (DEDM)

1. Ensures that the NRC Facility Security Program is operated in an efficient and effective manner consistent with existing policies and regulations, and in a manner that protects against identified threats.
2. Determines, as a Designated Approving Authority, along with the Office of the Chief Information Officer (OCIO), the adequacy of security protections for NRC automated information systems and for the information contained in those systems.

C. General Counsel (GC)

Performs legal review and provides legal advice on facility security-related matters.

D. Inspector General (IG)

1. Provides and/or coordinates with the Division of Facilities and Security (DFS), Office of Administration (ADM), when appropriate, any information developed or received relating to security and insider threat matters.

2. Supervises and conducts investigations and audits of NRC programs and operations, as authorized by the Inspector General Act, including allegations of misconduct or wrongdoing by agency employees and contractors.

3. Assists in law enforcement response on a case-by-case basis. Under normal circumstances, contract protective security officers (PSO), local police, and Federal Protective Service Police are the primary armed security and law enforcement response and will respond to situations in NRC buildings requiring an armed security officer. The Office of the Inspector General (OIG) GG-1811 series criminal investigators may be called upon to assist and are authorized by statute to carry a firearm, make an arrest without a warrant, and seek and execute warrants for arrest, search of premises, or seizure of evidence.

E. Director, Office of Administration (ADM)

1. Develops policies and procedures and manages the operation and maintenance of NRC offices, facilities, and equipment.

2. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC facility security program.

3. Develops and administers overall agency policy, direction, procedures, and inspection of NRC contractors, subcontractors, and grantee facility clearances related to the National Industrial Security Program.

4. Administers the Occupant Emergency Program (OEP), as carried out by DFS, ADM.

5. Serves as the Senior Agency Official (SAO) for the Insider Threat Program (ITP).

F. Director, Office of International Programs (OIP)

1. Provides information to DFS pertaining to foreign nationals visiting NRC facilities.

2. Coordinates with the Office of Nuclear Security and Incident Response (NSIR) for NRC employees who are scheduled to travel overseas to receive a travel briefing.

3. Coordinates with DFS for foreign nationals who plan to attend training.

G. Director, Office of Investigations (OI)

Maintains liaison with DFS and develops policy, procedures, and quality control standards for investigations of licensees, applicants, and their contractors or vendors, including the investigations of all allegations of wrongdoing by other than NRC employees and contractors. Refers substantiated criminal cases to the Department of Justice (DOJ).

H. Director, Office of Nuclear Security and Incident Response (NSIR)

1. Develops overall agency policy and provides management direction for licensee facility clearances, and evaluation and assessment of technical issues on matters pertaining to NRC licensee security.
2. Serves as the safeguards and security contact with the Department of Homeland Security (DHS), the intelligence and law enforcement communities, the Department of Energy (DOE), and other agencies on matters pertaining to NRC licensee security.
3. Administers the information security programs that deal with the classification and declassification of classified information through policy development, security classification guide approval, inspections, and security education/awareness activities.
4. Administers the NRC counterintelligence, Safeguards Information (SGI), secure telecommunications, foreign disclosure of information, and authorized classifier programs.
5. Serves as the safeguards and security contact, as well as the Protected Critical Infrastructure Information (PCII) contact with DHS, DOE, intelligence and law enforcement communities, and other agencies on matters pertaining to NRC licensee security and the NRC security program.
6. Acts as the NRC Central Office of Record for Communications Security (COMSEC) and operates the NRC's secure communications center.
7. Develops, maintains, and integrates NRC plans, procedures, and training for response to domestic and international radiological events and to any incidents that threaten the Continuity of Government (COG) or the NRC Continuity of Operations (COOP).
8. Informs foreign assignees of the sensitivity of SGI and the information security requirements in accordance with international agreements as authorized by the Commission and other applicable laws and regulations.

I. Chief Information Officer (CIO)

1. Administers the information security programs that deal with Sensitive Unclassified Non-Safeguards Information (SUNSI) through guidance, oversight, inspections, and security education/awareness activities.
2. Determines, as a Designated Approving Authority, along with the Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital Programs (DEDM), the adequacy of security protections for NRC automated information systems and for the information contained in those systems.

J. Chief Information Security Officer (CISO), Information Security Directorate (ISD), Office of the Chief Information Officer (OCIO)

Administers the cybersecurity programs for all levels of information through guidance, oversight, inspections, and cybersecurity education/awareness activities.

K. Office Directors and Regional Administrators

1. Ensure that NRC employees and NRC contractor personnel under their jurisdiction are aware of and comply with the provisions of this MD, as appropriate.
2. Advise DFS of the existence or proposed creation of any business relationship or interest that would require DFS review of any contract, subcontract, or similar action and of any significant change or termination of any classified or sensitive unclassified interests in organizations and functions under their jurisdiction.
3. Submit facility physical security plans to DFS for review and approval, which include location, purpose/nature of activity, classification level, access list, point-of-contacts (POCs), equipment needed, hardware/software to be used, operating procedures, hours of operation, contingency plan, maintenance procedures, etc.
4. Advise DFS, NSIR, or OCIO, whichever is appropriate, of any information that indicates noncompliance with this MD or that is otherwise pertinent to the proper protection of classified information, sensitive unclassified information, or NRC assets.
5. Take or direct action, as requested by DFS, or as otherwise may be pertinent, regarding deficiencies in security or property protection in facilities or functions under their jurisdiction.
6. Support and promote NRC security awareness for personnel under their jurisdiction, including ensuring that subordinate NRC supervisors discharge their responsibilities for on-the-job security education and awareness of their employees.
7. Support and implement the NRC Security Incident Program in all organizations and functions under their jurisdiction, including submitting all security incident reports to DFS.
8. Control and safeguard classified and sensitive unclassified information under their jurisdiction in accordance with applicable laws and this MD.
9. Make written requests to the Director of DFS, Director of NSIR, or Chief Information Officer (CIO) for exceptions to their respective requirements or deviations from this MD.
10. Appoint security advisors for NRC offices and regions who act as liaison between DFS and NRC staff within their respective offices or regions, and assist with security-related efforts at the direction of DFS.

L. Director, Division of Facilities and Security (DFS), ADM

1. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC Facility Security Program, including the approval of facilities for the handling and storage of classified and sensitive unclassified information.
2. Promotes NRC security awareness regarding physical and personnel security matters.
3. Administers the NRC Security Incident Program and coordinates action, as appropriate, with other NRC and Federal organizations regarding incidents of possible disclosure of classified information or other violations of Federal law or statutes.
4. Informs OIG of law enforcement, employee misconduct, and contractor wrongdoing matters, as appropriate.
5. Manages and implements the access control program for all NRC facilities.
6. Oversees the physical security protection of classified information.
7. Administers the ITP in coordination with other designated NRC offices.

IV. APPLICABILITY

The policy and guidance in this MD apply to all NRC staff and visitors to the NRC. Additionally, this policy and guidance are made applicable to certain contractors through the use of appropriate contract and purchase order provisions.

V. DIRECTIVE HANDBOOK

Handbook 12.1 contains guidelines and procedures with regard to facility security, the protection of classified information and facilities, safeguarding of NRC property and programs, promotion of NRC security awareness, administration of the Security Incident Program, and managing the NRC access control program.

VI. REFERENCES

Code of Federal Regulations

10 CFR Part 25, “Access Authorization.”

10 CFR Part 73, “Physical Protection of Plants and Materials.”

10 CFR 73.22, “Protection of Safeguards Information: Specific Requirements.”

10 CFR Part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data.”

10 CFR Part 160, “Trespassing on Commission Property.”

32 CFR Part 2001, “Classified National Security Information.”

32 CFR Part 2004, "National Industrial Security Program Directive No. 1."

41 CFR Part 101, "Federal Property Management Regulations."

41 CFR Part 102-74, Subpart C, "Conduct on Federal Property."

Department of Defense

National Industrial Security Program Operating Manual (NISPOM), Department of Defense 5220.22M, February 28, 2006, and Change 2, May 18, 2016.

Executive Orders

E.O. 10865, "Safeguarding Classified Information Within Industry," as amended, February 20, 1960.

E.O. 12829, "National Industrial Security Program," as amended, January 6, 1993.

E.O. 12968, "Access to Classified Information," as amended, August 2, 1995.

E.O. 13526, "Classified National Security Information," December 30, 2009.

E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011.

Department of Homeland Security

Interagency Security Committee (ISC) Standards.

Intelligence Community Directives

Intelligence Community Directive No. 705-1, "Sensitive Compartmented Information Facilities," May 26, 2010.

Intelligence Community Directive No. 705-2, "Standards for the Accreditation and Reciprocal Use of Sensitive Compartmentalized Information Facilities," September 17, 2010.

General Services Administration

General Services Administration Forms Library: http://www.gsa.gov/portal/forms/type/SF.

National Security Agency

Committee on National Security Systems (CNSSI) 4005, "Safeguarding COMSEC Facilities and Materials," August 22, 2011.

"National Security Agency (NSA)/Central Security Service (CSS) Evaluated Products List for High Security Crosscut Paper Shredders," May 18, 2015.

National Institute of Standards and Technology

FIPS PUB 201-2, Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013.

Nuclear Regulatory Commission

NRC Management Directives—

2.3, "Telecommunications."

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.4, "Release of Information to the Public."

5.13, "NRC International Activities Practices and Procedures."

11.1, "NRC Acquisition of Supplies and Services."

11.7, "NRC Procedures for Placement and Monitoring of Work With the U.S. Department of Energy (DOE)."

11.8, "NRC Procedures for Placement and Monitoring of Work With Federal Agencies Other Than U.S. Department of Energy (DOE) Laboratory Work."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.5, "NRC Cybersecurity Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

12.7, "NRC Safeguards Information Security Program."

NRC Forms Library:
http://fusion.nrc.gov/nrcformsportal/default.aspx.

Occupant Emergency Plan Web Site for NRC Headquarters and the Regional Offices:
http://drupal.nrc.gov/nrc/security-topics.

OEDO Procedure – 0450, Foreign and Domestic Travel Threat Response Process, June 1, 2016 (ML16103A268).

Office of Government Ethics Legal Advisory, LA-15-03, "The Standards of Conduct as Applied to Personal Social Media Use," April 9, 2015, available at https://www2.oge.gov/Web/OGE.nsf/0/16D5B5EB7E5DE11A85257E96005FBF13/$FILE/LA-15-03-2.pdf.

U.S. Department of Defense and U.S. Nuclear Regulatory Commission Memorandum of Understanding Concerning the National Industrial Security Program (NISP), April 2, 1996.

Presidential Decision Directives

Homeland Security Presidential Directive 3, "Homeland Security Advisory System," March 11, 2002.

Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

Presidential Decision Directive 63, "Critical Infrastructure Protection," May 22, 1998.

Underwriters Lab

Underwriters Laboratory (UL) Standard 2050.

United States Code

Americans with Disabilities Act (ADA) of 1990, as amended (42 U.S.C. 12101 et seq.).

Atomic Energy Act (AEA) of 1954, as amended (42 U.S.C. 2011 et seq.).

Communications Assistance for Law Enforcement Act of 1994 (CALEA) (47 U.S.C. 1001 et seq.).

Coordination of Counterintelligence Activities (50 U.S.C. 402a).

Crimes and Criminal Proceedings (18 U.S.C.).

Electronic Communications Privacy Act of 1986 (EPCA) (18 U.S.C. 2510 et seq.).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. 3541 et seq.).

Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

Freedom of Information Act (5 U.S.C. 552).

Homeland Security Act of 2002 (6 U.S.C. 101 et seq.).

Inspector General Act of 1978 (5 U.S.C. App. 3).

Privacy Act of 1974, as amended (5 U.S.C. 552a).

REAL ID Act-Title II, H.R. 1268, "Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief," 2005 (Pub. L. 109-13).

Title III, "Wire Interception and Interception of Oral Communications," of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. 2510 et seq.).

DH 12.1 NRC FACILITY SECURITY PROGRAM DT-16-39

Volume 12:	Security
Approved By:	Victor M. McCree Executive Director for Operations
Date Approved:	September 28, 2016
Expiration Date:	September 28, 2021
Issuing Office:	Office of Administration Division of Facilities and Security
Contact Name:	Denis Brady 301-415-5768

EXECUTIVE SUMMARY

Management Directive (MD) 12.1, "NRC Facility Security Program," is revised to incorporate new requirements of—

- Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."
- Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (FIPS PUB 201-2).
- The latest Interagency Security Committee (ISC) Standards.
- Other U.S. Nuclear Regulatory Commission policy changes related to physical security requirements.

This MD has been revised to facilitate ease of reference and for clarity. As a result, information from several sections (e.g., prior MD 12.1 section entitled "Facility Clearance and Surveys") have either been modified, removed, or reorganized. This revision reflects updates to sections regarding the Industrial Security Program; Security Incident Program; visitor procedures; Personal Identity Verification (PIV) cards; temporary visitor, employee, and contractor badges; Occupant Emergency Plan (OEP); security container management; security assessments and surveys; key and lock program; and controlled, administratively controlled, limited access, and security controlled areas. In addition, this revision incorporates the courier card process, onsite and offsite public meeting and hearing security support process, the REAL ID Act, Insider Threat Program (ITP), Protective Threat Assessment Team (PTAT), foreign and domestic travel threat response process, and Criminal History Program (CHP).

EXECUTIVE SUMMARY

This revision also incorporates recommended changes resulting from the Office of the Inspector General (OIG) Audit 16-A-10 regarding the standards for offices to appoint room owners (i.e., Access Reviewing Officials (ARO)) and notify the Office of Administration (ADM) of changes to access rights for limited access areas, and OIG Audit 12-A-12 regarding the restructured reporting process for safeguards information.

TABLE OF CONTENTS

EXHIBITS

I. GENERAL

The Division of Facilities and Security (DFS), Office of Administration (ADM), administers the U.S. Nuclear Regulatory Commission security program. DFS is responsible for protecting NRC facilities and personnel, and ensuring the safeguarding of classified and sensitive unclassified information at NRC and NRC contractor facilities. Additionally, DFS coordinates with law enforcement agencies on related matters and implements the Criminal History Program (CHP).

II. PHYSICAL SECURITY

A. Introduction

The NRC uses a defense-in-depth approach to the physical protection of its facilities that includes multiple layers of security to deter, detect, delay, and interdict adversarial actions and other undesirable events.

B. Physical Barriers

1. Physical barriers (e.g., walls, doors, fences, barricades, vehicle barrier systems, and electronic entry devices) are used to deny or impede unauthorized access to the facility and other areas as required in the Interagency Security Committee (ISC) Standards or as determined by DFS. Permanent physical barriers are used to enclose all controlled, administratively controlled, limited access, and security controlled areas. Barriers shall not be moved, manipulated, destroyed, or otherwise altered in any manner by unauthorized individuals.

2. Electronic and electro-mechanical devices (i.e., card readers) are used and approved by DFS to control personnel access. These devices limit access to only those individuals authorized to enter a given area. DFS manages and determines access to NRC facilities.

C. Actions on Government Property

1. Section 229 of the Atomic Energy Act (AEA) of 1954, as amended, and Title 10 of the *Code of Federal Regulations* (CFR) Part 160, prohibit the unauthorized entry, carrying, transporting, introducing, or causing to be introduced, of any dangerous weapon, explosive, or other instrument or material that is likely to produce substantial injury or damage to persons or property, into or upon any designated facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Commission. If violations occur, the statute contains a section regarding penalties for these actions.

2. The General Services Administration (GSA), "Rules and Regulations Governing the Conduct on Federal Property," are posted at entrances to NRC facilities in accordance with 41 CFR Section 102-74, Subpart C, to provide reasonable assurance of notice to persons entering. (See GSA rules and regulations available at http://www.gsa.gov/graphics/ogp/Fed_Rules_Regs8_5x11_Final2005_R27-s10_0Z5RDZ-i34K-pR.pdf.) All individuals in or on NRC property must comply with all official signs of a prohibitory, regulatory, or directory nature and with the lawful direction of Federal police officers and any other authorized individual in accordance with 41 CFR 102-74.

3. Photography on NRC Property

   (a) Staff may not use personal or other devices to film, record, or photograph the following: Personal Identity Verification (PIV) cards, NRC badges, or other forms of identification; security equipment (e.g., cameras, barriers, screening equipment, etc.); protective security officers (PSOs); NRC employees, visitors, or contractors without clear permission from the individual(s); or sensitive equipment or information in any form.

   (b) NRC staff are responsible for all photographs that are taken, posted, and/or disseminated. Staff should be mindful of their social media posting and representation of themselves, coworkers, and the agency. (See Office of Government Ethics Legal Advisory, LA 15-03, "The Standards of Conduct as Applied to Personal Social Media Use," April 9, 2015.)

   (c) Contractors and visitors are required to receive prior approval from the Director of DFS to take photographs inside NRC facilities. Requests for approval must be submitted using NRC Form 875, "Request for Authorization to Use a Camera and/or Video Recording Devices in U.S. NRC Facilities and Space." If the visitor is a member of the media, the Office of Public Affairs (OPA) will coordinate with DFS regarding the use of camera and/or video recording devices. The submitting

individual is responsible for informing the photographer of the applicable NRC requirements and restrictions. Additionally, submission of an NRC Form 875 alone does not constitute approval.

D. Access Control System

The NRC access control system is managed and maintained by DFS. It is used to ensure that only authorized individuals are granted physical access. Access lists (a list of individuals with authorized access) are required for administratively controlled, limited access, and security controlled areas and must be reviewed and approved by the room's designated owner (i.e., the Access Reviewing Official) at least annually. An Access Reviewing Official (ARO) is designated by his or her respective branch chief and is responsible for overseeing the general operations of the room and providing DFS with an access list for individuals requiring authorized access. The access list must be updated by the ARO when there are any personnel and/or ARO changes. The ARO must notify DFS within 3 business days of the change, unless otherwise noted in the area's security plan. The office must notify DFS within 3 business days if a new ARO needs to be appointed, changed, or modified. At a minimum, DFS will annually update the access list.

E. Intrusion Detection and Assessment System

All entrances to the facility and general perimeter have intrusion detection equipment. Alarm signals are sent to both the Federal Protective Service (FPS) and the NRC's Central Alarm Station (CAS). The alarms are monitored by the PSOs who execute the duties of the alarm station operator(s) at each facility. As deemed necessary by DFS, PSOs will assess and survey all alarm areas and other locations by using authorized surveillance equipment and/or by conducting inspections. Upon arrival, all individuals are subject to authorized surveillance in common areas.

F. Protective Security Officers (PSOs)

The NRC uses armed PSOs to ensure the physical protection of NRC Level III and IV facilities, its personnel, and information. Staff and visitors to NRC facilities are required to comply with direction given by any PSO.

G. Keys and Locks

DFS manages the NRC's key and lock program that includes keys to the facilities, areas within the buildings, doors, etc. This does not include keys for general furniture in staff offices or cubicles (e.g., desk drawer cabinets and flip cabinets). Keys shall not be created, destroyed, distributed, and/or reproduced without explicit approval and coordination with DFS.

H. Security Container Management

DFS maintains control of security containers at the NRC. This includes lock-bar cabinets and material destruction bins (burn bins), and GSA-approved containers. Relocation, repair, or any alteration of the security container's condition must be coordinated with DFS. (See Sections II.I and II.J of this handbook.) Only those containers approved and managed by DFS are allowed to be used to store NRC information and property.

I. Lock-Bar Cabinets

Lock-bar cabinets must be secured with a DFS provided lock and may store designated information up to and including safeguards information (SGI) within NRC facilities in accordance with NRC Management Directive (MD) 12.6, "NRC Sensitive Unclassified Information Security Program"; MD 12.7, "NRC Safeguards Information Security Program"; NRC Yellow Announcement YA-05-0077, "Policy Revision: NRC Policy and Procedures for Handling, Marking, and Protecting Sensitive Unclassified Non Safeguards Information (SUNSI)," October 26, 2005 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML051220278); and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements." Staff may obtain a lock for a container by creating a ticket through the NRC Service Catalog and completing the required information.

J. General Services Administration (GSA)-Approved Containers (Safes)

1. GSA-approved containers (i.e., safes) may store up to and including Secret (S), National Security Information (NSI), and Restricted Data (RD) when located outside of an area not approved for open storage of classified information. When not in use, all classified information must be stored in a GSA-approved Class 6 container or a room approved for open storage of classified information and/or systems. MD 12.1 neither applies to nor controls the storage or protection of Top Secret Information. For more information on how to handle classified information and Top Secret information, please see MD 12.2, "NRC Classified Information Security Program."

2. Staff must contact DFS to request a GSA-approved container by following the procedures detailed in Section II.J.7(a). A GSA-approved container shall not be moved or relocated without prior coordination with DFS or the regional security advisor, if applicable.

3. Control of the container's combination must be in compliance with MD 12.2 and may not be disseminated to anyone not listed on the Standard Form (SF) 700, "Security Container Information," (see Exhibit 1 of this handbook) that is affixed to the inside of the container. Additional SF 700s should be used if more than 4 individuals require the combination, in compliance with Section II.J.4 of this MD, to the security container. A copy of any additional SF 700s must be provided to DFS and should indicate the number of SF 700s in use, as well as the sequence in which the new form would fall. (See Exhibit 1 of this handbook.) Individuals are prohibited from annotating container combinations, unless the combinations are stored at the level of

information contained therein. For example, if the container holds Secret level information, the written combination to that container must be protected as if it were a Secret document as well.

4. All individuals requiring access to the container must possess a security clearance at the same level or higher than the highest classification or designation of material within the container and have a need-to-know. A need-to-know is a determination by a person having responsibility for protecting or holding the sensitive information, be it classified information, safeguards information, or sensitive unclassified information, that a proposed recipient's access to the sensitive information is necessary in the performance of an official and lawful requirement. Knowledge of, possession of, or access to sensitive information including classified, safeguards, and/or sensitive unclassified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance. The designated owner must be listed as the primary point-of-contact (POC) for the container on the SF 700.
5. A copy of the SF 702, "Security Container Check Sheet," must be completed and posted outside of all GSA-approved containers in use, regardless of the safe's contents. (See Exhibit 2 of this handbook.) The SF 702 must be filled out each time the container is opened, closed, or checked.
6. Regardless of the level of the information in the container, each GSA-approved container that is in use must have a DFS-approved security plan stored in the container.
7. The following are procedures for requesting a GSA-approved container, changing a container combination, transferring the container to a new owner, relocating the container, removing a container from use, and reporting an unsecured container.

   (a) Requesting a GSA-Approved Container

   NRC staff should create a ticket request through the NRC Service Catalog and complete the required information. A member from DFS will then contact the requester regarding the container. In an NRC regional location, staff should contact the security advisor and follow local office procedures.

   (b) Changing a Container's Combination

   The safe owner shall request a change in the container's combination, if any of the following conditions exist:

   (i) A new container is received;

   (ii) Access by an authorized person is no longer required (e.g., the individual has left the agency or is on assignment in another office or division);

   (iii) The container combination has possibly been compromised (i.e., unauthorized disclosure of the combination is suspected);

(iv) The container is no longer needed;

(v) The container is found damaged or unsecured; or

(vi) Once every three years, if the conditions listed above have not occurred.

(c) Transferring a GSA-Approved Container to a New Owner

(i) The current owner must inventory the contents and determine if any items can be destroyed or declassified. The owner must properly destroy or transfer the contents in accordance with applicable MDs and any other requirements. If assistance is needed, please contact DFS for direction or proper destruction methods. If items should be reviewed for declassification, contact the Nuclear Security and Incident Response, Information Security Branch (NSIR/ISB), for additional assistance.

(ii) The current owner must work with his or her management to determine who will be designated as the new owner of the container. Once a new owner has been determined, that individual becomes responsible for any of the container's existing and new contents. The individual must read and sign the container's security plan and immediately contact DFS to have the combination changed by following the procedures listed in Section II.J.7(b) of this handbook. Failure to have the combination changed after the container is transferred shall result in a security incident, infraction, or violation.

(d) Relocating a Container

The owner of the container must complete an NRC Form 30, "Request for Administrative Services," and submit it to Property and Labor Services Branch (PLSB), Associate Directorate for Space Planning and Consolidation (ADSC), ADM, with a copy to FacilitiesSecurity.Resource@nrc.gov, KeysandLocks.Resource@nrc.gov, and the regional security advisor, if appropriate. The form must contain information regarding the existing location of the container, its container number (located on a plaque above the lock), and the location to where it will be moved.

(e) Removing a GSA-Approved Container from Active Use

If removing a container from active use, the owner of the container must ensure that all contents are properly destroyed or transferred and that the container is completely empty of all material. The owner must then coordinate with DFS to get the combination reset and verifying that the container is empty. After the combination has been reset, the owner must complete an NRC Form 30 to remove the container from use. Before submitting the NRC Form 30, DFS must reset the combination. Failure to do so may result in the container not being removed.

(f) Reporting an Unsecured Container

The container owner must complete an NRC Form 183, "Report of Security Incident," if he or she finds the container unsecured. The container owner must conduct an inventory of all items and submit written verification of all items' accountability as soon as possible. An NRC staff member, even if not the container owner, upon discovering the container unsecured, should immediately contact the CAS and not leave the container unattended until a PSO or a member of DFS arrives. Then, the reporting staff member should complete an NRC Form 183 by the next business day.

K. Protection of Classified Information In Use, Storage, and Reproduction of Classified Information

1. Introduction

(a) This section provides the practices and procedures for the protection of classified information pursuant to the AEA of 1954, as amended; the Energy Reorganization Act of 1974, as amended; pertinent Executive Orders (e.g., E.O. 13587 and 12968, as amended); and 32 CFR Part 2001, "Classified National Security Information."

(b) Each Federal agency must establish controls to ensure that classified information is used, stored, processed, reproduced, transmitted, or destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons. As it relates to protecting classified information, physical security includes physical access controls and administrative procedures used to adequately deter its unauthorized disclosure. DFS, ADM, maintains and oversees these controls. Nothing in this MD shall be construed to contradict or inhibit compliance with NRC policy, laws, and building codes applicable to safety and the Americans with Disabilities Act of 1990, as amended.

2. The factors to be taken into consideration in determining the type and degree of physical protection afforded classified information include the level of the classified information, such as Top Secret (TS), Secret, or Confidential; relative vulnerability of that information to espionage, sabotage, theft or other unlawful actions; and need for compartmentalization of the information.

3. Protection of Classified Information in Use

(a) Access controls must be established to provide adequate protection and prevent access by unauthorized persons to classified information.

(b) Access to classified information must be limited to persons who possess the appropriate access authorization and who require access to the information in the performance of their official government duties or contractual obligations

(i.e., need-to-know). A need-to-know is a determination by a person having responsibility for protecting or holding the sensitive information, be it classified information, Safeguards Information (SGI), or sensitive unclassified information, that a proposed recipient's access to the sensitive information is necessary in the performance of an official and lawful requirement. Knowledge, possession of, or access to, sensitive information including classified, safeguards, and/or sensitive unclassified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance. For more information on the electronic processing of classified information, please see MD 12.5, "NRC Cybersecurity Program."

(c) A person without appropriate access authorization for the area visited or the information contained in that area must be escorted at all times by an authorized NRC staff member while within a security area or any other area in which unsecured classified information is located, such as an open storage area. Additionally, when there are local or unique restrictions on access because of operating, technical, or compartmentalization consideration, only a person knowledgeable of these restrictions shall serve as an escort.

4. Storage of Classified Information

All classified information up to and including Secret-RD must be stored in a GSA-approved container (safe) when not in use or in a DFS-approved room certified for open storage.

5. Reproduction of Classified Information

(a) In accordance with 32 CFR 2001.45 (b), reproduction of classified information shall be held to a minimum, consistent with operational requirements.

(b) Reproduction shall only be conducted by authorized individuals knowledgeable of the procedures for classified reproduction and only on DFS-approved copy machines or in DFS-approved spaces. Copies of any classified information shall be protected using the same controls as the original version.

(c) See MD 12.2, "NRC Classified Information Program," for information regarding how to prepare and transmit/mail classified information.

L. Destruction of Sensitive and Classified Material

1. Documents

Receptacles (e.g., shredders) have been placed throughout NRC facilities to provide staff with a means to properly destroy information up to and including Secret-RD. DFS must review, label, and approve any cleared receptacles in order for them to be used for destruction of sensitive or classified information. All categories of SUNSI can be destroyed by using a burn bin or by any means approved by the Office of the

Chief Information Officer (OCIO) for the SUNSI program. When a burn bin is full and needs to be emptied, staff should call the CAS and provide the burn bin location to the PSOs.

(a) SGI can be destroyed using any of the approved destruction measures described in MD 12.7, "NRC Safeguards Information Security Program." This includes shredders that are DFS-approved to destroy classified information and burn bins.

(b) Classified information up to and including Secret-RD must be destroyed using a DFS-approved and labeled shredder. A shredder must meet the National Security Agency (NSA) standards for destruction of classified information in order to be approved for such use. TS and Sensitive Compartmented Information (SCI) information must be controlled and properly destroyed by the Top Secret Control Officer. (See MD 12.2 for additional details.)

2. Electronic Media

(a) Any electronic media (i.e., compact discs (CDs), thumb drives, hard drives) containing sensitive information up to and including Secret-RD, must be brought or shipped using the proper methods of transmission for the classification level directly to an FSB staff member for destruction and should not be left unattended. Staff should remove all electronic media from its case (i.e., CD case or hard drive cover) before submitting it for destruction. All sensitive and classified media intended for destruction, must be routed through FSB and shall not be disposed of in the shredders or burn bins, unless provided DFS-approved equipment for destruction of electronic media. Electronic media containing TS and SCI must be controlled and properly destroyed by the TS Control Officer. (See MD 12.2 for additional details.) For additional information regarding the destruction of classified electronic media, please see MD 12.5.

(b) Staff must protect electronic media in accordance with the level of information contained therein, even though the device will be destroyed.

3. NRC staff must coordinate with DFS in advance when a large quantity (i.e., larger than a moving box worth of material) of sensitive material needs to be destroyed.

M. Controlled, Administratively Controlled, Limited Access, and Security Controlled Areas

1. Controlled Area or Space

An area of an NRC facility where an individual has passed through a perimeter security access control, for example, NRC personnel using their PIV cards to enter the facility or a visitor clearing the visitor screening process. An NRC-controlled area is accessible by all badged individuals and screened visitors.

2. Administratively Controlled Area

   An area within NRC-controlled space where access needs to be limited for a specific operational purpose. The area must have designated Access Reviewing Officials (AROs) who manage the access list to the area and provide it to DFS. The list must be, at a minimum, reviewed and approved by a designated ARO annually.

3. Limited Access Area

   An area within NRC-controlled space that has restricted access due to the type of operations, equipment, and information, and/or is required by ISC Standards. Access is limited to staff who have the appropriate clearance or access authorization and a need-to-know. The area must have designated AROs who manage the access list to the area and provide it to DFS. The list must be, at a minimum, reviewed and approved annually by a designated ARO.

4. Security Controlled Access Area

   An area within NRC-controlled space that processes, stores, and/or is used to discuss classified information including any Sensitive Compartmented Information Facility (SCIF). Access is limited to staff who have the appropriate clearance and a need-to-know. The area must have an approved security plan and/or be accredited by a Cognizant Security Agency (CSA) (e.g., NRC, Department of Energy (DoE), Department of Defense (DoD)). A security controlled access area that processes, stores, and/or is used to discuss classified information at the collateral level must be constructed to Intelligence Community Directive (ICD) Number 705 standards. The area must have designated AROs who manage the access list to the area and provide it to DFS. The list at a minimum must be reviewed and approved annually by a designated ARO.

III. SECURITY ASSESSMENTS AND SURVEYS

A. NRC Facilities

DFS conducts security reviews and assessments of all NRC facilities in accordance with the latest Department of Homeland Security ISC standards. Assessment results provide insight into any needed security improvements and are appropriately documented and reviewed by DFS management.

B. Secure Rooms

1. All new secure rooms within the NRC are constructed to meet the ICD 705 and 32 CFR Part 2001.43 standards to ensure the rooms can be used to their highest capability to support NRC's mission. All secure rooms are designated as security controlled areas and can be cleared up to the Secret-RD level. See MD 12.5 for information regarding electronic processing of information. Each room has a security plan that describes the room's classification level, security procedures, and

restrictions, as well as its own access list that is updated at least annually by the ARO. Only those who have read and signed the security plan and those on the access list are allowed unescorted access into the room. All requirements within the room's security plan must be followed. Any failure to do so must be reported immediately to DFS and may result in a security incident, infraction, or violation.

2. All secure rooms must have a documented assessment on an annual basis.

   (a) DFS will conduct the assessments annually for secure rooms at NRC headquarters.

   (b) NRC regional locations will have annual assessments conducted by the designated security advisors and/or DFS.

IV. VISITOR REQUIREMENTS

A. Introduction

1. All visitors and non-badged contractors requiring access to an NRC facility must be processed through security, registered in the Visitor Access Request System (VARS) by an NRC staff member, and present valid picture identification to enter any NRC facility.

2. NRC staff members expecting visitors in law enforcement who might be armed must notify and coordinate with DFS or their regional security advisor in advance. Failure to do so may result in a delay or denial of the visitor's entry into an NRC facility.

B. Visitor Hours

1. Visitors are allowed at NRC facilities between the hours of 6:00 a.m. and 6:00 p.m. and must adhere to all posted signage, NRC policies, and instructions given by authorized individuals. Visitors should not be present on NRC property after 6:00 p.m. unless given prior authorization by DFS.

2. Weekend visits must be approved by DFS in advance of the visit. Failure to coordinate in advance may result in the denial of the visitor's entry into an NRC facility.

C. Visitor Access Request System (VARS)

1. The NRC POC for the visitor must enter him or her into the VARS and include all appropriate information before the visitor arrives at the NRC facility.

2. If onsite parking is required for the visitor(s) a parking pass may be selected within the VARS entry. Vehicle information should be provided, if known.

3. If the visitor is a foreign national, the appropriate country code must be selected. The United States shall not be selected as the country of origin for any foreign national visitor. If the foreign visitor has a visa, it must be presented along with his or her passport upon entry. For more information regarding visits by foreign nationals, see Section XIV of this handbook.

D. Screening Process

1. All visitors and non-badged contractors must be screened through security before entering an NRC facility. All individuals remain subject to search and authorized surveillance upon arrival. Federal agencies may, at their discretion, inspect packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons (occupants) arriving on, working at, visiting, or departing from Federal property in accordance with General Service Administration Rules and Regulations Governing Conduct on Federal Property (41 CFR 102-74.370).
2. Very Important Person (VIP) visitors, who are designated by the Office of Protocol, Chairman's office, or Commission offices as approved by DFS, may be granted expedited screening. The specific terms of this process are coordinated with the NRC host office and DFS. VARS entries, screening, and visitor badging are still required. VIP visitors should bring their confirmation of VIP status to the NRC facility to expedite the screening process.

E. Temporary Visitor Badges

1. A visitor will be issued a temporary visitor badge after being screened through security. At a minimum, the temporary visitor badge will contain the following information: visitor's name, NRC POC and phone number, and clearance level. This badge must be prominently worn at all times and visitors must be under continuous escort by a badged NRC staff member or other badged person approved by DFS. If visiting NRC headquarters, the temporary visitor badge is valid for use between the buildings but the visitor must be screened upon each entry.
2. Upon completion of the visit, the visitor must be escorted to a public access area where the visitor's badge shall be returned to a PSO before departure from the facility. This badge is one-time use only and cannot be used for another visit.

F. Escort Requirements

A visitor must be under continuous escort by an authorized NRC staff member while in NRC-controlled space. Only five visitors are allowed to be escorted by a single NRC employee or approved contractor. An escort is not required when in an area designated as publicly accessible. On a case-by-case basis, DFS may authorize a contractor to escort. An escort must adhere to all established escort policies.

G. Foreign National Visitors

If the foreign national has a visa in addition to a passport, the NRC POC must send a copy of both documents to ForeignVisitor.Resource@nrc.gov with the date, location, topic or agenda for the visit, and the NRC POC for the visit at least 12 business days, when possible, in advance of a foreign national visiting any NRC facility. Additionally, the visitor's NRC POC must register the visitor in VARS with the appropriate country code

before the individual arrives. See Section XIV.D of this handbook for more information regarding preparing for a visit from a foreign national.

V. PERSONAL IDENTITY VERIFICATION CARDS (PIV), TEMPORARY BADGES, AND COURIER CARDS

A. PIV Card Issuance

1. All NRC employees, select contractors, and other individuals, as determined by the NRC and DFS, who require access to NRC facilities are issued an identification badge called a Personal Identity Verification (PIV) card. PIV cards are compliant with Homeland Security Presidential Directive (HSPD)-12 requirements. The use of PIV cards aids in access control for NRC facilities to ensure that only authorized persons gain entry. PIV cards also indicate any access limitations to classified information, limited, security, or other areas.
2. An individual who is issued a PIV card (cardholder) will be provided a compliant badge holder in which the PIV card must be kept. The badge holder must meet the security requirement derived from the Federal Information Processing Standards (FIPS) 201-2 standard and the supporting National Institute of Standards and Technology (NIST) special publication. This aids in protecting the PIV card against any unauthorized access to information stored on the badge.

B. PIV Cardholder Responsibilities

1. Badged individuals must prominently wear their badge at all times while in NRC-controlled space and keep their badge in a compliant badge holder.
2. It is each individual's responsibility to maintain control of his or her PIV card or badge and ensure that it is protected from compromise, theft, and is not loaned to anyone for any reason.
3. When outside NRC-controlled areas, a badged individual is required to conceal his or her badge and ensure it is physically protected. Additionally, it shall not be copied, replicated, or photographed for any purpose.
4. All cardholders must read and sign the, "Privacy Act Statement Issuance of NRC Personal Identity Verification Card," agreement upon issuance.
5. A cardholder must report immediately to DFS any loss, theft, compromise, or other non-compliance with the PIV card user agreement in accordance with Section VIII of this handbook.

C. Temporary Badges for Employees and Contractors

NRC staff, including contractors, who forget their PIV card may be issued a temporary access card (badge) for the day. This badge will allow the individual general access to the facility from 6:00 a.m. - 6:00 p.m., but if special access is needed to a particular area, the individual must contact DFS. Individuals issued a temporary access card must return it to the security desk before they leave the facility the same day.

D. Courier Cards

Any NRC staff member requesting a courier card in order to transport classified information must complete the NRC Form 90, "Classified Courier Card Application and Approval," and receive approval from DFS. A courier card is valid for up to 3 years or until the need to transport classified information ends, and must be returned to DFS. When carrying classified material, staff must ensure that the classified material is not transported in a container that obviously displays that the information contained therein is classified. A courier card is not required to transport classified information between NRC headquarter buildings. See MD 12.2 for more information regarding the requirements for carrying classified material.

E. Badge and PIV Card Confiscation

A PSO or member of DFS may confiscate an NRC-issued PIV card or badge if DFS deems it necessary to deny the individual access to any NRC facility. Confiscation of an NRC-issued PIV card or badge may be done at the discretion of DFS. This confiscation does not necessarily denote revocation of employment or security clearance.

F. Terminated Contractors

1. A contracting officer's representative (COR) must collect the PIV card from a contractor who is no longer active on an NRC contract immediately upon his or her termination or severance and notify DFS of the separation. Additionally, the COR must notify DFS if he or she is aware that the contractor will be beginning a new contract. The COR must arrange for the immediate return of the PIV card to DFS or may place it in the designated drop boxes located in the lobbies of each headquarters building. If located in a regional office, the COR should return the badge to their designated security advisor. Failure to do so will result in a security incident, infraction, or violation in accordance with Section VIII of this handbook.
2. If the contractor held a security clearance, the COR must also ensure that the contractor completes the Standard Form 312, "Classified Information Nondisclosure Agreement," upon termination and returns the completed form to DFS.

VI. ONSITE AND OFFSITE PUBLIC MEETING/HEARING SECURITY SUPPORT

A. Onsite Security Support

1. Unclassified Meetings

   (a) The NRC office hosting the meeting/hearing must submit an NRC Form 876A, "Request for Security Support at On-site U.S. NRC Public Meetings/Hearings," at least 15 business days in advance of the event in order to coordinate with DFS or, if appropriate, the regional security advisor for security support.

   (b) Escort responsibilities apply to all NRC staff members and it is the responsibility of the host office to ensure all requirements are followed.

   (c) The host office should enter expected visitors into VARS to ensure timely processing and screening. Unanticipated visitors will be entered into VARS by the PSOs after screening and processing. All visitors must comply with posted regulation and instruction of all authorized individuals.

2. Sensitive Unclassified Non-Safeguards Information or Safeguards Information Meetings

   (a) Public meetings or hearings involving subject matter categorized as SUNSI or SGI must be coordinated with DFS in advance to ensure that appropriate security measures are in place. An NRC Form 876A is required; however, no SUNSI or SGI material should be included or contained in the form.

   (b) All attendees in an SGI meeting must have their access authorization verified by the entity that granted their access to SGI. The meeting POC must obtain verification of the attendee's access on official letterhead from the granting entity and indicate that the attendee has a need to know the information in the meeting.

3. Classified Meetings/Hearings and Conversations

   (a) Meetings or hearings involving subject matter categorized as classified must be coordinated with DFS in advance to ensure appropriate clearance, need-to-know, and other security measures are in place. DFS will coordinate with NSIR, as appropriate. An NRC Form 876A is required for all onsite classified meetings when non-NRC staff are in attendance; however, no classified matter should be included or contained in the form.

   (b) The Director of DFS must approve the location of all classified meetings/conferences, hearings, and/or conversations not taking place in a DFS-approved secure space or SCIF.

   (c) All attendees in a classified meeting must have their clearance verified through DFS in advance. Failure to do so may result in delay or denial from attending the classified meeting.

B. Offsite Security Support

1. DFS contracts and coordinates security support for offsite public meetings or hearings with local law enforcement at the request of the NRC host office. The NRC host office must request security support at least 30 business days in advance by completing and submitting the NRC Form 876B, "Request for Security Support at Off-site U.S. NRC Public Meetings/Hearings," and NRC Form 877, "U.S. NRC Security Support Supplement for Public Meetings/Hearings." Failure to do so may result in limited security support.
2. DFS must be consulted before venue selection and, if deemed necessary by DFS, representatives from DFS may attend the meeting or hearing in order to facilitate coordination with local law enforcement.

VII. SECURITY AWARENESS

A. Security Debriefings for Exiting Employees

1. An NRC employee or temporary NRC employee who is leaving the NRC must complete a security debriefing with DFS, or the NRC regional security advisor if applicable, on his or her last day and surrender their NRC-issued PIV card before exiting the facility. This briefing must be conducted in person and should be scheduled at least 1 week before the employee's departure from the NRC, unless exigent circumstances exist in which case DFS should be contacted as soon as possible to coordinate alternative procedures.
2. The employee must bring the NRC Form 270, "Separation Clearance," and Personal Evacuation Kit (PEK) with them to the security debriefing. During the security debriefing, the employee will read and complete the SF 312, "Classified Information Nondisclosure Agreement" (available in the GSA Forms Library at http://www.gsa.gov/portal/forms/type/SF), and the NRC Form 136, "Security Termination Statement" (available in the NRC Forms Library at http://fusion.nrc.gov/nrcformsportal/default.aspx).

B. Security Advisor Program

1. All NRC office directors or regional administrators must select a primary and alternate security advisor and subsequently submit this information to DFS. If the security advisors change, DFS must be notified by memorandum as soon as possible.
2. The role of a security advisor is to support NRC staff knowledge of and compliance with security policies and procedures. Security advisors act as liaisons between DFS and NRC staff within their respective offices or regions and assist with other security-related efforts at the direction of DFS.
3. DFS will keep all security advisors apprised of any pertinent information regarding security policies, procedures, or other events.

4. Regional Security Advisors are responsible for—

   (a) Enrollment, activation, termination, and collection of PIV cards.

   (b) Key and lock program for their region.

   (c) Liaison with the FPS.

   (d) Physical access control system administrator.

   (e) Liaison to DFS for security incidents, security system concerns, issues, and/or repairs.

   (f) Assist with other security related efforts at the direction of DFS.

VIII. SECURITY INCIDENTS, INFRACTIONS, AND VIOLATIONS

A. Introduction

Deviation from NRC policies may result in a security incident, infraction, or violation.

B. Security Incidents

A security incident results when there is a failure to comply with NRC security requirements or procedures not involving classified material. Some examples of security incidents include the following:

1. Loss of or failure to return an NRC-issued PIV card or badge;
2. Leaving sensitive unclassified documents or material unattended, unsecured, or improperly stored;
3. Improper transmission of sensitive unclassified documents or material;
4. Allowing an unauthorized person access to sensitive unclassified information;
5. Failure to safeguard a sensitive unclassified combination;
6. Failure to properly escort visitors; and
7. Failure to follow a DFS-approved security plan that does not involve classified information.

C. Security Infractions

A security infraction results when there is a failure to comply with NRC security requirements or procedures that involve classified material. Some examples of security infractions include the following:

1. Leaving classified documents or material unattended, unsecured, or improperly stored;
2. Improper transmission of classified documents or material;

3. Improperly marking, storing, and/or handling of classified information;
4. Allowing an unauthorized person access to classified information;
5. Leaving a classified security container unattended and unsecured;
6. Failure to properly safeguard a classified combination; and
7. Repeated failure to adhere to a DFS-approved security plan.

D. Reporting Security Incidents and Infractions

1. An NRC employee shall report all security incidents or infractions immediately following their occurrence or observed occurrence by completing and submitting the NRC Form 183, "Report of Security Incident." If necessary, the initial report to DFS may be made orally, but must be finalized in writing by submitting the NRC Form 183 to DFS. A report should not contain any SGI or classified information, unless the report is protected according to the level of information involved when transmitted or verbally communicated to DFS through an authorized secure telecommunications system or secure information technology (IT) system. A security incident may be initially reported by telephone to 301-415-6885, or online at http://drupal.nrc.gov/content/report-safety-or-security-incident. For information regarding computer security incidents, please see MD 12.5.
2. A contractor shall immediately report a security incident or infraction to DFS and send a copy to the NRC project officer and/or COR and the regional security advisor, if appropriate. The report must include the details of the incident or infraction, as well as the name of the person who committed it. If the contractor does not have the capability to complete and submit the NRC Form 183, the COR must do so on behalf of the contractor.
3. The NRC Form 183 must contain the following:
   (a) The full name of the individual involved;
   (b) The individual's office and title, or if a contractor, the company and COR's name;
   (c) The classification of the information involved, but not the vulnerability if it has not been corrected; and
   (d) The date, reason or cause, and nature of the incident or infraction.

E. Review of Reports or NRC Form 183

1. Regional staff members should forward a report of the security incident or infraction and the NRC Form 183 directly to DFS. Regional staff should also send a copy to the regional security advisor when submitting the report or information.
2. DFS will review the report and follow up with the reporting individual if additional information or action is needed. An individual responsible for a security incident or

infraction may be subject to mandated training regarding the information about the specific security incident or infraction and/or possible disciplinary action.

3. All infractions will be referred to the Personnel Security Branch (PSB) in DFS.
4. If warranted, DFS will forward the report to OIG or the Office of Investigations (OI) for consideration.

F. Security Violations

1. Scope of Violations

   Breach of the following provisions may constitute a criminal violation:

   (a) AEA of 1954, as amended;

   (b) International Security Act of 1950, when related to NRC activities;

   (c) Title 18 U.S. Code relating to:

      (i) Espionage or information control, Sections 792-98;

      (ii) Sabotage, Sections 2151-57;

      (iii) Treason, sedition, and subversive activities, Sections 2381-85;

      (iv) Malicious mischief, Sections 1361-64;

      (v) Actual or threatened use of explosives against persons or property, Sections 841-48;

      (vi) Destruction of Government property, Sections 1361 and 2232;

      (vii) Embezzlement and theft, Sections 641-665;

      (viii) Extortion and threats, Sections 871-878, and

   (d) Other pertinent Federal statutes or regulations.

2. Reporting Procedures

   (a) All NRC staff, including NRC regional staff and contractors, shall immediately report all suspected violations, including any suspicious or unusual behavior, directly to DFS. The report may be made orally but must be finalized in writing by submitting the NRC Form 183 to DFS and send a copy to the regional security advisor, if applicable.

   (b) After submitting the report, no additional action is to be taken unless directed by DFS, OIG, and/or OI.

   (c) DFS will coordinate with and support OIG and OI, as necessary, during this process.

(d) Content of Report

(i) A report that contains classified or sensitive unclassified information must be properly protected and marked with the appropriate classification and control markings.

(ii) A report of a suspected violation not involving a loss or compromise of classified or sensitive unclassified information discussed in Section VIII.E of this handbook must contain a statement regarding the items and information involved, names of staff involved, circumstances surrounding the violation, and action contemplated or taken.

3. Investigation of Violations

(a) OIG is responsible for investigating and referring any alleged or suspected violation by an employee of the NRC or an NRC contractor to the Federal Bureau of Investigation (FBI), as necessary. OIG may elect to initially defer or conduct joint fact-finding activities with DFS.

(b) OI is responsible for investigating and referring to the FBI any alleged or suspected violation that a licensee, applicant for an NRC license, and their contractors and vendors commit, as necessary.

(c) The NRC will provide assistance to all law enforcement agencies, as appropriate, but coordination with DFS, OIG, or OI is required.

(d) NRC followup will include appropriate coordination with the FBI or other law enforcement authorities, as well as OIG or OI, as needed.

4. Records

(a) DFS, NSIR, OIG, and OI will maintain records, as appropriate, of all instances involving the loss or compromise of classified information. The records must identify the classified information involved, the date on which the loss was discovered or the compromise occurred, any action taken to determine whether the loss or compromise could reasonably be expected to cause damage to national security, the determinations reached, a copy of the damage assessments in cases of loss or compromise, and any other action taken in each instance.

(b) An agency head or senior agency official shall notify the Director of the Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), when a violation occurs under 32 CFR 2001.48, to comply with the reporting requirements specified in Sections 5.5(b)(1), (2), or (3), of Executive Order (E.O.) 13526.

IX. INSIDER THREAT PROGRAM (ITP)

A. In accordance with E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," and NRC policies, the NRC developed and implemented an Insider Threat Program (ITP). (See Federal Register Notice at https://www.gpo.gov/fdsys/granule/FR-2016-02-25/2016-04026.)

B. The ITP is led by ADM and supported by various other offices within the NRC that form the Insider Threat Assessment Team (ITAT). The ITAT facilitates communication and efforts in the event an insider threat is reported.

C. An insider threat is defined as the threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through the unauthorized disclosure of classified or safeguards information. Any suspected or known insider threat should be reported immediately to ADM by sending an e-mail to InsiderThreatProgram.Resource@nrc.gov. The e-mail should provide general information, including the suspected nature of the threat or concern and the reporting individual's contact information. Upon receipt of the report, ADM or another ITP-affiliated office may request additional information.

X. PROTECTIVE THREAT ASSESSMENT TEAM (PTAT)

The NRC's Protective Threat Assessment Team (PTAT) consists of individuals from select offices responsible for providing a quick coordinated assessment and response to any threat that is reported to DFS that may potentially impact NRC employees, officials, or facilities. The PTAT makes an immediate assessment, determines appropriate agency response, obtains approval of agency response from NRC management, and implements the response in coordination with internal and/or external officials or entities.

XI. FOREIGN AND DOMESTIC TRAVEL THREAT RESPONSE PROCESS

The foreign and domestic travel threat response process is a process that advises agency management of safety, security, and threat-related information in order to make a risk-informed decision for NRC staff planning for or currently on official foreign and/or domestic travel. The Threat Advisory Group (TAG) is an interdisciplinary group that consists of experts in physical security, international programs, and threat assessment. Executive Director for Operations (EDO) Procedure-0450, "Foreign and Domestic Travel Threat Response Process," established the TAG, that—

A. Provides a coordinated review and assessment of law enforcement information, travel advisories and alerts from the Department of State and the Department of Homeland Security, intelligence threat-related information regarding foreign and domestic travel, and

B. Provides a recommendation to the EDO to make a risk-informed decision regarding official agency staff travel.

XII. PROHIBITIONS ON WIRETAPPING AND EAVESDROPPING DEVICES

A. Introduction

Section XII relates to surreptitious use of wiretapping or eavesdropping devices in conversations or wire (including wireless) transmission without the consent of any of the participants. For NRC policies and procedures related to consensual monitoring or recording of verbal or wire communications, see MD 2.3, "Telecommunications."

B. Procurement and Use of Devices

1. NRC funds must not be used to purchase wiretapping or eavesdropping devices, except as stated below. These devices must not be installed or used for eavesdropping or wiretapping in or on any NRC building, or installation, or on real estate owned or leased by the U.S. Government for the use of the NRC, except as authorized by law. See Title III of the Omnibus Crime Control and Safe Streets Act of 1968, "Wire Interception and Interception of Oral Communications," and the Foreign Intelligence Surveillance Act of 1978.
2. Title III provisions, codified at Title 18, *United States Code*, Section 2512, prohibit the manufacture, distribution, sale, possession, or advertising of interception devices whose primary purpose is the surreptitious interception of wire, oral, or electronic communications. Violations of this statute are punishable by a fine and a period of imprisonment of not more than 5 years. The purpose of this provision is to limit the availability of interception devices to authorized law enforcement entities and to telecommunications carriers and to keep them out of the hands of unauthorized eavesdroppers.

XIII. OCCUPANT EMERGENCY PLAN

A. Purpose

The purpose of the NRC's Occupant Emergency Plan (OEP) is to reduce the possibility of personal injury and facility damage in the event of an emergency that affects the NRC's facilities. The OEP applies to all building occupants, including employees, contractors, and visitors, and also describes what to do in events such as fires, bomb threats, medical emergencies, and other varying conditions. DFS is responsible for the development and implementation of the OEP at NRC headquarters. The Technical Training Center (TTC) and regional offices must follow the template provided and submit their OEP for approval by DFS.

B. Personal Evacuation Kits (PEKs)

PEKs are issued to all NRC employees and are available for contractors working at NRC facilities. The PEKs provide some essential items to use in the event of a building emergency. The NRC employee or contractor is responsible for periodically inspecting

their PEK. If items need replacing, regional staff members should contact their security advisor, and headquarter staff members should contact DFS.

XIV. FOREIGN NATIONAL PROGRAMS

A. Introduction

All foreign nationals who come to an NRC facility shall be considered, without exception, one of the following: foreign assignee, foreign trainee, or foreign visitor. The following section describes DFS's role in the various foreign national programs.

B. Foreign Assignee Program

1. A foreign assignee is an individual from an international regulatory authority that is sponsored by either his or her country or the International Atomic Energy Agency (IAEA) and assigned to the NRC for an extended period of time, consistent with applicable policies and other formal agreements. For information regarding foreign assignees, see MD 5.13, "NRC International Activities, Practices, and Procedures," and MD 12.3, "NRC Personnel Security Program."

2. DFS reviews, evaluates, and approves the foreign assignee's assignment, invitation letter, and security plan in coordination with the Office of International Programs (OIP) and the host office before the arrival of the foreign assignee. DFS must be notified of any change to the foreign assignee's anticipated arrival date or travel to another NRC facility or NRC licensee facility.

3. All modifications, amendments, or changes to any portion of the documents regarding the assignment shall be reviewed and approved by DFS before implementation. DFS must be notified if the foreign assignee is approved for access to SUNSI, SGI, or classified information, as authorized by the Commission and international agreement and implemented by OIP and NSIR. DFS will provide guidance to OIP and the host office for drafting the security plan when the assignment involves access to SGI and SUNSI. Failure to comply with, or any unauthorized deviation from, the foreign assignee's security plan may result in a security incident, infraction, or violation to the host office and any other individual(s) as deemed necessary by DFS upon review of the situation.

4. After coordination with OIP, DFS will issue the foreign assignee a badge upon arrival. The assignee must return his or her badge to OIP on the last day of the assignment at the NRC. OIP will return the badge to DFS immediately. The assignee will not be allowed to retain, photograph, or otherwise duplicate the badge.

C. Foreign Trainee Program

1. Foreign nationals who are registered and plan to attend an NRC-sponsored training course are considered foreign trainees.

2. The OIP foreign trainee coordinator will provide DFS with the NRC Form 122 "Security Plan"; a copy of the individual's passport and visa, if the foreign trainee has a visa in addition to a passport; and the NRC Form 70A, "Request for Name Check" for review and approval.
3. Upon receipt of results from the NRC Form 70A, DFS will review the NRC Form 122, and make a determination. Once approved, DFS will send copies of the NRC Form 122 to the appropriate parties identified on the form. If results are not received before the start of training, DFS will coordinate with OIP to make a determination on how to proceed.
4. For detailed information regarding foreign nationals attending NRC sponsored-training, see MD 5.13.

D. Foreign Visitor

1. Any other foreign national coming to the NRC shall be considered a foreign visitor, unless the requirements for the Foreign Assignee Program or Foreign Trainee Program are met.
2. Before a visit from a foreign national, the NRC POC for the visit must do the following:
   (a) Notify the appropriate OIP desk officer of the pending visit.
   (b) Enter the visitor's name into VARS and select the appropriate country code.
   (c) If the foreign national has a visa in addition to a passport, the NRC POC must obtain a copy of both no less than 12 business days in advance of the visit. Passports and visas contain personal information and must be protected in the same manner as Personally Identifiable Information (PII).
   (d) Send a copy of the passport and visa to ForeignVisitor.Resource@nrc.gov with a copy to the appropriate security advisor if at a region or the TTC, along with the following information:
      (i) Date(s), time(s), and location(s) of the visit;
      (ii) Purpose of the visit, topics to be discussed, or visit agenda;
      (iii) NRC POC name and phone number for the visit;
      (iv) Level of information to be discussed at the meeting (e.g., publicly available, SUNSI, SGI, and/or classified);
      (v) The OIP desk officer informed of the visit; and
      (vi) If needed, request for security support.

3. The foreign visitor will be screened through security and provided a visitor badge upon entering the building and must be escorted at all times in NRC-controlled space. Additionally, the foreign visitor cannot take pictures and/or video recordings in NRC-controlled space. (See Section II.C.3 of this handbook.) Any suspicious activity or behavior must be reported to DFS immediately.

XV. INDUSTRIAL SECURITY PROGRAM

A. Introduction

1. Cleared U.S. industry entities (industrial, educational, commercial, or other entity) are granted a facility security clearance (FCL) when they have a legitimate need to access classified information to develop and produce nuclear and defense technology. The National Industrial Security Program (NISP) was established by E.O. 12829, as amended, to ensure that cleared U.S. industry properly safeguard any classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. Under E.O. 12829, as amended, the NRC is designated as one of the five NISP CSAs for the Federal Government. NSIR is responsible for all NRC licensees who fall within 10 CFR Part 95, “Facilities Clearance and Safeguarding of National Security Information and Restricted Data.”

2. As a CSA, the NRC is required to grant FCLs and provide oversight and assistance for any and all contractor entities working on a classified contract or interagency agreement issued on behalf of the NRC. Classified contracts or interagency agreements include those requiring access to Confidential, Secret, and TS-NSI along with any associated contract or agreement caveats such as Restricted Data and Formerly Restricted Data. DFS is responsible for carrying out the mission of NISP implementation and overseeing the day-to-day functions on behalf of the NRC.

3. A contractor facility or any other type of designated legal operating entity in private industry or a college/university, must have a legitimate need for access to classified information in connection with a U.S. Government or foreign government requirement, such as the award of a classified contract or other agreement, in order to participate in the NISP. When a contractor is granted an FCL, regardless of the granting CSA, the contractor must abide by the governing rules and regulations of the latest NISP Operating Manual (NISPOM) as set forth in DoD 5220.22-M.

4. In order for DFS to determine if a contractor needs an FCL associated with an NRC contract or interagency agreement, a COR must complete and submit to DFS an NRC Form 187, “Security Contract and/or Classification Requirements,” for review and approval to IndustrialSecurity.Resource@nrc.gov before solicitation for bid or proposal. The COR should maintain a copy of the approved NRC Form 187 for his or her records.

B. Facility Security Clearances

1. FCL with Reciprocity - Multiple CSAs

   (a) In instances where a contractor already holds an FCL with another CSA, such as DoD or DoE, DFS may grant FCL reciprocity with another CSA. This effectively relieves NRC of its NISP security oversight responsibilities to prevent duplicate oversight efforts of the contractor.

   (b) Alternatively, if DFS and another CSA agree, NRC may become the CSA with oversight of the contractor, depending on the situation.

   (c) In cases where FCL reciprocity is granted, regardless of who becomes the CSA with oversight, the contractor will fall under the active direction of the lead CSA's industrial security program and will be afforded the same level of protection that NRC or another CSA would give under the requirements of the NISP. The CSAs will communicate with each other in order to determine who will be the lead CSA for the contractor.

2. FCL with No Reciprocity - NRC as the Sole CSA

   (a) In a case where the NRC is the sole CSA to grant a classified contract or other agreement requiring the issuance of an FCL, the in-process contractor will undergo a survey process in which DFS will collect corporate documents from the contractor and conduct research in order to determine if the contractor is eligible for an FCL. Upon completion of the survey process, DFS will make a decision whether to issue an FCL to the contractor.

   (b) When a contractor is granted an FCL, they may immediately begin working on the classified contract.

   (c) If an FCL is not approved, the contractor will not be authorized to perform work on the contract until actions have been taken to correct the issue(s) preventing the FCL from being granted. If DFS determines the issues are uncorrectable, DFS will not award an FCL.

3. Storage and Transmission of Classified Information

   If a contractor needs to store, transmit, or process classified information at their site, the contractor must first put the necessary requirements in place before being granted authority to do so. After a contractor has implemented all necessary requirements, "safeguarding" authorization may be granted as part of the FCL award.

C. Facility Security Clearance Oversight

1. Security Vulnerability Assessments

   (a) DFS will conduct recurring onsite security vulnerability assessments (SVAs) of each contractor awarded an FCL for work on an NRC classified contract. Contractors with non-possessing FCLs (no classified storage at the contractor's

location) will be assessed approximately every 2 years, and possessing contractors (granted "safeguarding") will be assessed approximately every year, starting from the date the FCL was first issued. During the SVA, vulnerabilities will be cited for each area where a contractor does not meet the requirements of DoD 5220.22-M, and enhancements will be granted for areas where a contractor goes above and beyond the requirements of DoD 5220.22.

(b) A rating matrix that will take into account the number of enhancements and vulnerabilities will be used to determine one of the following five (5) ratings for a contractor: Superior, Commendable, Satisfactory, Marginal, Unsatisfactory. The contractor's rating will be addressed in an SVA report completed by DFS and include specific details of the SVA. After the SVA, the contractor will be required to report to DFS how each vulnerability cited during the SVA was addressed.

(c) Three additional types of SVAs that DFS is authorized to conduct are compliance SVAs, closeout SVAs, and unannounced SVAs. Compliance SVAs will be conducted after a contractor receives a rating of less than Satisfactory on their regularly scheduled SVA. Closeout SVAs will be conducted when a possessing contractor is being terminated, regardless of the reason for termination, in order to ensure all classified material is returned to the NRC or accounted for prior to terminating the FCL. Unannounced SVAs may be conducted to address a specific or immediate problem, concern, or deficiency.

2. Facility Security Clearance Change Conditions

Contractors will notify DFS of any changes to their company or personnel that may impact their FCL, as some change conditions at a contractor facility may affect the contractor's ability to maintain an FCL. Depending on the significance of the change, DFS will take action to record and, if necessary, mitigate any negative effects a change may have on a contractor's FCL, as best as possible. Some change conditions may potentially result in the invalidation, revocation, or termination of a contractor's FCL if the change is not mitigatable or if a contractor is uncooperative with meeting the mitigation requirements, as set forth by DFS.

D. Facility Security Clearance Termination

1. FCL Termination

The COR must notify DFS when a classified contract ends and ensure that the contractor badges have been collected, if applicable. DFS will terminate an FCL when a contractor has completed its NRC classified activities or no longer requires access to NRC classified information. Before FCL termination, DFS will ensure that classified information at the contractor site has been appropriately destroyed or returned to NRC custody, as applicable.

2. FCL Invalidation

   In the event of a sub-satisfactory SVA rating or the failure of a contractor to abide by NRC guidance to correct a vulnerability, an FCL may be invalidated. While in an invalidated status, the contractor may continue to work on their current classified contracts but will not be allowed to bid on any additional classified contracts. FCL invalidation may be lifted once the NRC required actions are corrected.

3. FCL Revocation

   If a contractor has created a security concern great enough to warrant the removal of its FCL, the FCL will be revoked, and all classified work from the contractor will immediately stop.

4. FCL Termination Letter

   When an FCL is terminated or revoked, a termination letter will be mailed to the contractor as confirmation, and the contractor's file folder is to be maintained for a minimum of 2 years in the event the contractor re-enters the NISP.

5. Termination of Contractor Employee Access Authorizations

   Any contractor employees who no longer require NRC access authorization due to termination of an FCL, will be removed from access and properly debriefed.

XVI. CRIMINAL HISTORY PROGRAM (CHP)

In accordance with 10 CFR Part 73, "Physical Protection of Plants and Materials," the NRC maintains the CHP to facilitate fingerprint submissions for a criminal history record check between the licensees, applicants, certificate holders, and the FBI. This process is needed for those individuals requiring access to a product or a facility subject to regulation by the Commission or safeguards information. Fingerprint submissions are received by CHP either electronically or by hardcopy of the Civil Fingerprint Card (FD-258). Furthermore, the CHP facilitates submissions to the FBI's Electronic-National Instant Criminal Background Check System (e-NICS) for licensees, applicants, and certificate holders who require it for compliance with Commission orders and/or regulations.

EXHIBITS

Exhibit 1 Standard Form 700, "Security Container Information"

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

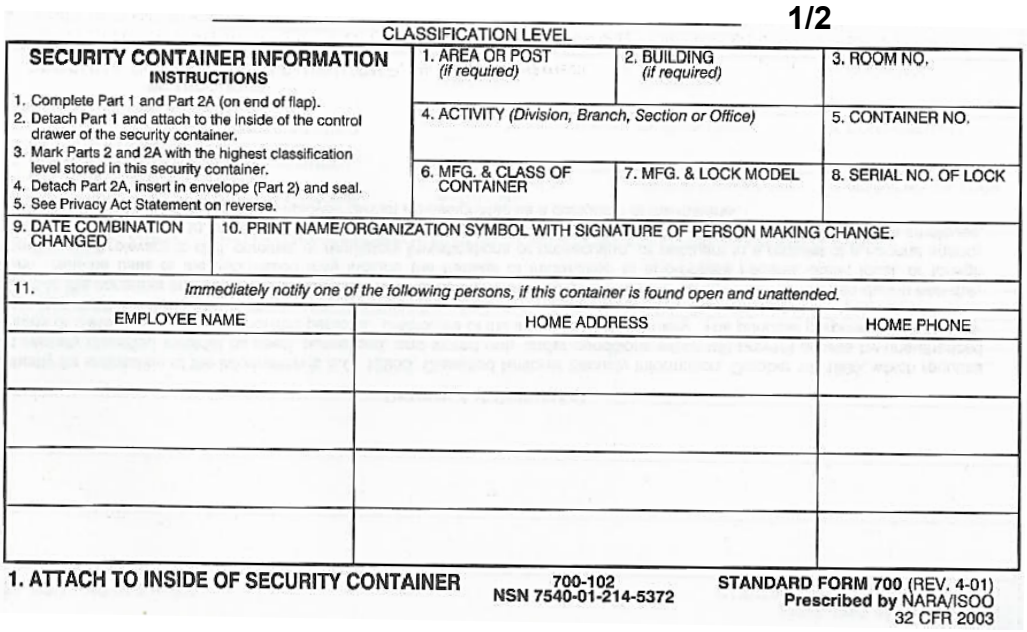
1. ATTACH TO INSIDE OF SECURITY CONTAINER 700-102 NSN 7540-01-214-5372 **STANDARD FORM 700** (REV. 4-01) **Prescribed by** NARA/ISOO 32 CFR 2003

Privacy Act Statement

Authority for solicitation of the information is E.O. 12958, Classified National Security Information, October 14, 1995, which requires that security classified material be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unauthorized persons. Disclosure of the information is voluntary. The principal purpose of the information is to provide on the inside of the security container the name, home address, and telephone number of employees who have access to the container and are custodians of the material so that they may be alerted if a container is found open during non-duty hours. Routine uses of the information may include the transfer of information to appropriate Federal, State, local, or foreign agencies when relevant to civil, criminal, or regulatory investigations or prosecution; or pursuant to a request of a Federal agency in connection with the hiring or retention of an employee, the issuance of a security clearance, or the investigation of an employee. If the information is not provided, the employee cannot be designated as a custodian of the material.

Exhibit 1 Standard Form 700, "Security Container Information" (continued)

If more than 4 individuals require the combination to the security container, additional SF 700s should be utilized in compliance with Section II.J.4 of this directive. A copy of any additional SF 700s must be provided to DFS and should indicate the number of SF 700s in use as well as the sequence in which the new form would fall.



1/2

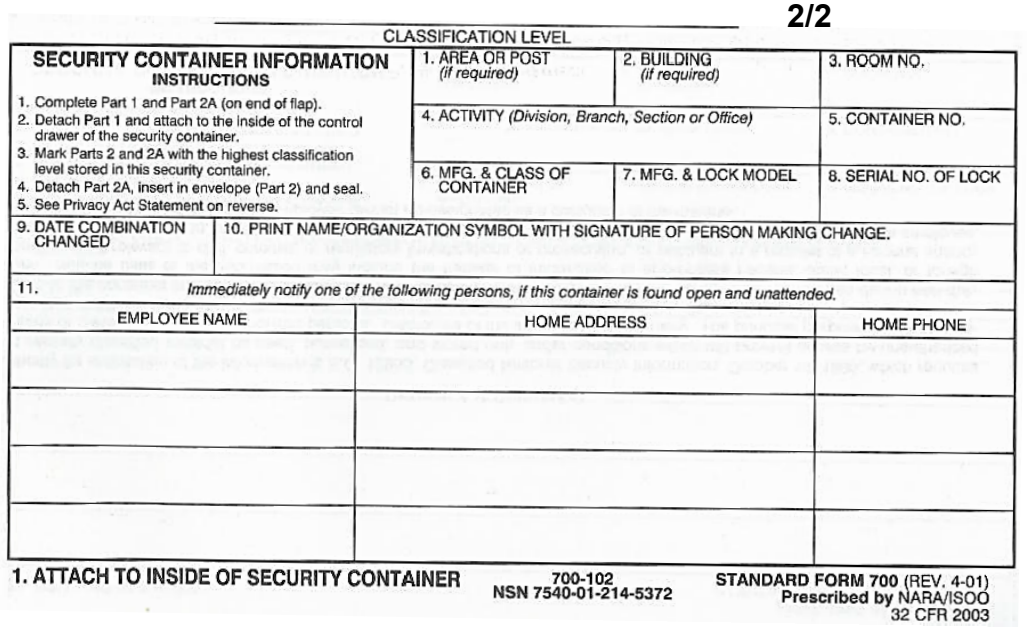
CLASSIFICATION LEVEL

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



2/2

CLASSIFICATION LEVEL

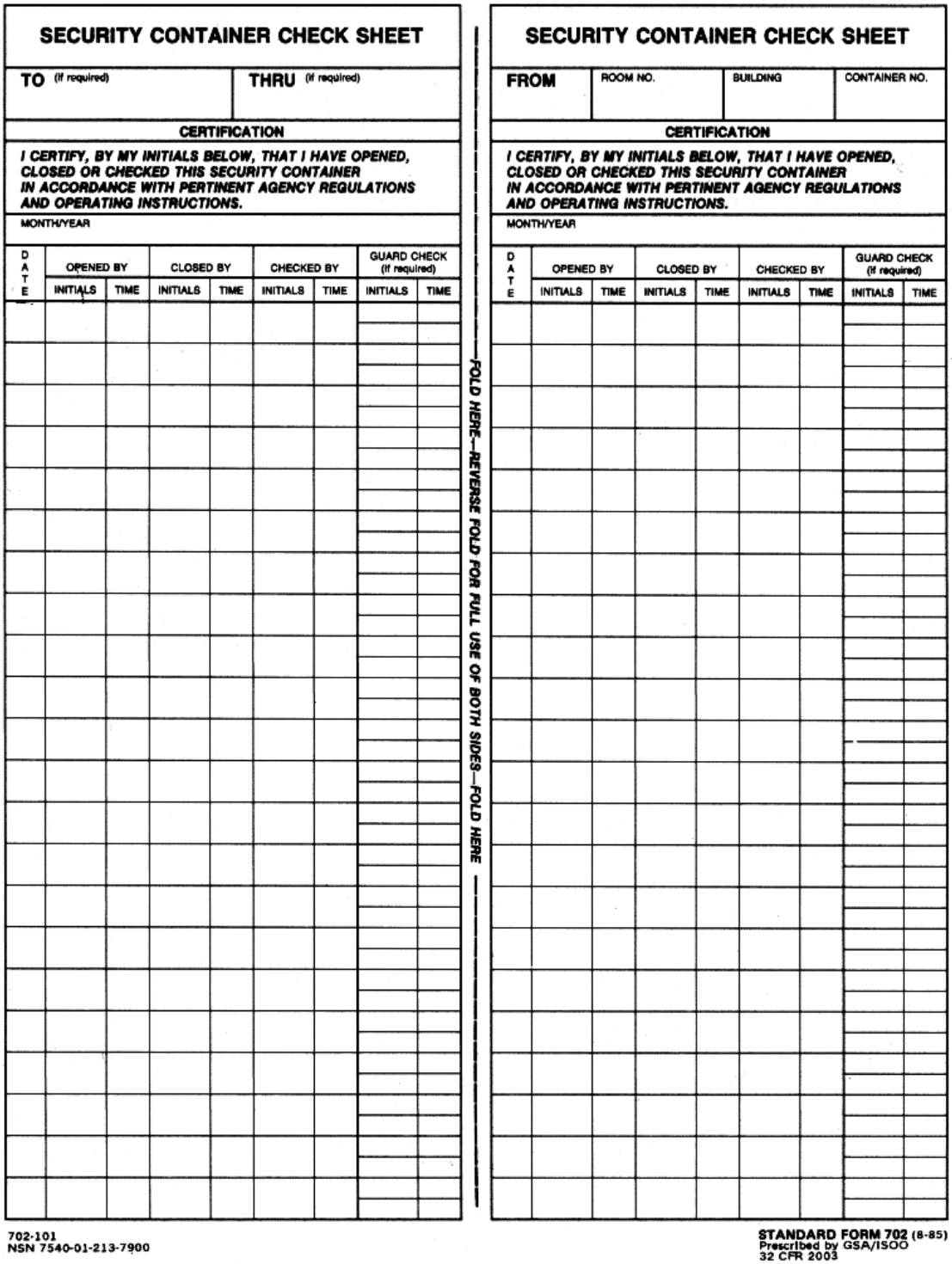
SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. Complete Part 1 and Part 2A (on end of flap). 2. Detach Part 1 and attach to the inside of the control drawer of the security container. 3. Mark Parts 2 and 2A with the highest classification level stored in this security container. 4. Detach Part 2A, insert 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

Exhibit 2 Standard Form 702, "Security Container Check Sheet"



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

702-101
NSN 7540-01-213-7900

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003