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

MD 12.1	NRC FACILITY SECURITY PROGRAM	DT-24-06
Volume 12:	Security	
Approved By:	James C. Corbett, Acting Director Office of Administration	
Date Approved:	April 22, 2024	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Michael England	

EXECUTIVE SUMMARY

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

- Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (FIPS PUB 201-3).
- The current Department of Homeland Security, "Interagency Security Committee (ISC) Standards."
- U.S. Nuclear Regulatory Commission policy changes related to physical security requirements.
- Replace the term Foreign with the term International.
- Removed references to Criminal History Program, see MD 12.3 for applicable information.

In addition, the NRC has revised this MD as part of its efforts to use more inclusive language in its publications. These changes, which include changing "Chairman" to "Chair" in some instances, are purely editorial and do not affect the meaning of the guidance in this document.

TABLE OF CONTENTS

I. POLICY

It is the policy of the U.S. Nuclear Regulatory Commission (NRC) 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)

Oversees 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 premises, or seize evidence.

E. Director, Office of International Programs (OIP)

1. Provides information to DFS about international visitors to NRC facilities.
2. Coordinates with the Office of Nuclear Security and Incident Response (NSIR) to provide a travel briefing for NRC employees who are scheduled to travel overseas.
3. Coordinates with DFS for international visitors who plan to attend training.

F. 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 implements 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).

G. Director, Office of Investigations (OI)

1. Coordinates with DFS to develop policy, procedures, and quality control standards for investigations of licensees, applicants, and their contractors or vendors, including the investigation of all allegations of wrongdoing by other than NRC employees and contractors.
2. 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 incident that threatens 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 Controlled Unclassified Information (CUI) through guidance, oversight, inspections, and security education/awareness activities.

2. Determines, as a Designated Approving Authority, along with the 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), Cybersecurity & Infrastructure Security Division (CISD), 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 the NRC Facility Security Program, as appropriate.

2. Advise DFS of the existence or proposed creation of a business relationship or interest that would require DFS review of a contract, subcontract, or similar action, and of a significant change or termination of a classified or sensitive unclassified interest in an organization or function under their jurisdiction.

3. Submit to DFS for review and approval facility physical security plans, which include location, purpose/nature of activity, classification level, access list, points-of-contact (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 the NRC Facility Security Program or that is otherwise pertinent to the proper protection of classified information, controlled unclassified information, or NRC assets.

5. Take or direct action, as requested by DFS, or as otherwise may be pertinent, to address 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 the requirements of the NRC Facility Security Program as described in this MD.
9. Make written requests to the Director of DFS, Director of NSIR, or CIO for exceptions to their respective requirements or deviations from requirements of the NRC Facility Security Program as described in this MD.
10. Appoint security advisors for NRC offices and regions who act as a 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 controlled 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 actions, 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 applicable to certain contractors based on their contract and purchase order provisions.

V. DIRECTIVE HANDBOOK

Handbook 12.1 contains guidelines and procedures regarding 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 117, "National Industrial Security Program Operating Manual (NISPOM)."

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."

41 CFR Part 102-81, "Physical Security."

Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Interagency Security Committee (ISC) Standards: https://www.cisa.gov/resources-tools/groups/interagency-security-committee-isc/policies-standards-best-practices-guidance-documents-and-white-papers.

Items Prohibited in Federal Facilities: An Interagency Security Committee Standard (series): https://www.cisa.gov/resources-tools/resources/isc-standard-items-prohibited-federal-facilities.

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP): https://www.cisa.gov/resources-tools/resources/isc-standard-risk-management-process.

Appendix A: The Design-Basis Threat Report (FOUO).

Appendix B: Countermeasures (FOUO).

Appendix C: Child-Care Center Level of Protection Template Implementation Guidance (FOUO).

Executive Orders

10865, “Safeguarding Classified Information Within Industry,” as amended, February 20, 1960.

12829, “National Industrial Security Program,” as amended, January 6, 1993.

12968, “Access to Classified Information,” as amended, August 2, 1995.

13526, “Classified National Security Information,” December 30, 2009.

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

14111, “Interagency Security Committee,” November 27, 2023.

Federal Register Notice

"Nuclear Regulatory Commission Insider Threat Program Policy Statement" (February 25, 2016, 81 FR 9519).

Intelligence Community Directives

Intelligence Community Directive No. 701, “Unauthorized Disclosures of Classified National Security Information,” December 22, 2017.

Intelligence Community Directive No. 705, “Sensitive Compartmented Information Facilities,” May 26, 2010.

Intelligence Community Standard No. 705-1, “Physical and Technical Security Standards for Sensitive Compartmented Information Facilities,” September 17, 2010.

Intelligence Community Standard No. 705-2, “Standards for the Accreditation and Reciprocal Use of Sensitive Compartmentalized Information Facilities,” December 22, 2016.

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, version 1.5, IC Tech Spec – for ICD/ICS 705.

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 201-3 (series), Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors," January 2022.

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 Controlled Unclassified Information (CUI) Program."

12.7, "NRC Safeguards Information Security Program."

12.8, "NRC Defensive Counterintelligence Program."

NRC Forms Library:
https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

Occupant Emergency Plan Web Site for NRC Headquarters and the Regional Offices:
https://usnrc.sharepoint.com/SitePages/Security-Topics.aspx.

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://www.oge.gov/web/oge.nsf/0/195DAE83D38EF6A9852585BA005BEC69/$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, "National Industrial Security System Certification."

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-24-06
Volume 12:	Security	
Approved By:	James C. Corbett, Acting Director Office of Administration	
Date Approved:	April 22, 2024	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Michael England	

EXECUTIVE SUMMARY

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

- Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors" (FIPS PUB 201-3).
- The current Department of Homeland Security, "Interagency Security Committee (ISC) Standards."
- Other U.S. Nuclear Regulatory Commission policy changes related to physical security requirements.
- Replace the term Foreign with the term International.
- Removed references to Criminal History Program, see MD 12.3 for applicable information.

In addition, the NRC has revised this MD as part of its efforts to use more inclusive language in its publications. These changes, which include changing "Chairman" to "Chair" in some instances, are purely editorial and do not affect the meaning of the guidance in this document.

TABLE OF CONTENTS

I. GENERAL

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

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 Physical Access Control Systems (PACS)) 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. The statute contains a section regarding penalties for violating 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, "Conduct on Federal Property," to provide reasonable assurance of notice to persons entering. (See GSA rules and regulations available at https://www.gsa.gov/cdnstatic/GSA_Rules_Reg_1105.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); protective security officers (PSOs); NRC employees, visitors, or contractors; or sensitive equipment or information in any form.

   (b) NRC staff are responsible for all photographs that are taken, posted, and 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. NRC Form 875 is available in the NRC Forms Library in SharePoint at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

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 (ARO)) at least annually. The ARO is designated by their 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 an intrusion detection system (IDS). 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. If an employee believes they are the subject of suspicious activity or behavior, they must make a report to DFS immediately.

F. Protective Security Officers (PSOs)

1. The NRC uses armed PSOs to ensure the physical protection of NRC Level III and IV facilities, its personnel, and information. PSOs will follow their FPS post orders and NRC Facility Security Plan orders that are contained in a separate protected Controlled Unclassified Information (CUI)-Security document. The NRC Facility Security Plan will identify security-related responsibilities—

   (a) Define building-specific security policies;

(b) Contain emergency contacts;

(c) Detail response procedures for emergencies;

(d) Outline approved protocols for access by employees, contractors, and visitors;

(e) Establish changes in security operations due to temporary upgrades in the National Terrorism Advisory System;

(f) Outline the security measure testing schedule performed by the security manager at facilities;

(g) Detailed Life Cycle Management for security equipment; and

(h) Identify critical and sensitive areas within the facility.

2. A copy of the NRC Facility Security Plan is required to be maintained at each post and will be provided to the PSOs by the contracting officer's representative (COR). 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, and keys for general furniture in staff offices or cubicles (e.g., desk drawer cabinets and flip cabinets). Keys shall not be created, destroyed, distributed, or reproduced without approval from and coordination with DFS.

H. Security Container Management

1. DFS maintains control of security containers at the NRC. This includes lock-bar cabinets and GSA-approved security 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 security containers approved and managed by DFS are authorized to be used to store NRC information and property.

2. NRC's regional management will appoint in writing a primary and alternate security container custodian who will be solely responsible for the security containers in their region. DFS must receive a copy of the appointment memo. The security container custodians are responsible for communicating to DFS anything dealing with the security container, including ensuring the combination is changed at the appropriate time, escorting the locksmith to conduct repairs or upgrades, and responding to any incident of the security container being left unsecure. Only the security container custodians can change the security container combination.

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 Controlled Unclassified Information (CUI) Program," and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements." Staff can get 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 Security Container (Safes)

1. GSA-approved security 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 security container, or a Security Controlled Area (SCA) approved by DFS for open storage of classified information and/or systems.

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

3. All individuals requiring access to a security container must possess a security clearance at the same level or higher than the highest classification or designation of material within the security container, have a signed non-disclosure agreement (NDA) SF-312, "Classified Information Nondisclosure Agreement," on file and have a need-to-know. A need-to-know is required for access to specific classified information to perform or assist in a lawful and authorized Government function (Executive Order (E.O) 13526, "Classified National Security Information"). SF-312 is available in GSA Forms Library website at https://www.gsa.gov/reference/forms/classified-information-nondisclosure-agreement-1.

4. Standard Form (SF)-700, "Security Container Information," is used for maintaining a record for each container, or vault, or secure room, used for storing classified information or systems. Complete all blocks on the form and the form must be updated each time the security container combination is changed.

   (a) Part 1 of SF-700 is not classified but contains personally identifiable information (PII) such as names, addresses, and telephone numbers that shall be protected by sealing Part 1 in an opaque envelope (not provided as part of the SF-700) conspicuously marked "Security Container Information" and stored on the inside of the security container of the locking drawer in accordance with SF-700 instructions. If the information must be accessed during non-duty hours and a new opaque envelope is not available to replace the opened one, the original

envelope should be temporarily resealed, to the extent possible, until Part 1 can be placed in a new envelope the next workday.

(b) Part 2 of SF-700, when completed, is classified at the highest level of classification authorized for storage in the security container. It shall be sealed and stored in accordance with SF-700 instructions. The classification authority block shall state, "Derived From: 32 CFR 2001.80(d)(3))," with declassification upon change of combination.

5. Standard Form (SF)-701, "Activity Security Checklist," provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability if irregularities are discovered. The SF-701 will be posted near the exit of the open SCA, to be completed when leaving the area. SF-701 is available in the GSA Forms Library website at https://www.gsa.gov/reference/forms/activity-security-checklist.

6. A copy of the SF-702, "Security Container Check Sheet," must be properly filled out and posted outside all GSA-approved security containers, regardless of the security container's contents. The opening and closing of the security container must be annotated on the SF-702 each time the security container is opened, closed, and for end-of-day checks. SF-702 is available in the GSA Forms Library website at https://www.gsa.gov/reference/forms/security-container-check-sheet.

7. Optional Form (OF)-89, "Maintenance Record for Security Containers/Vault Doors," is used to record the maintenance and preventive maintenance performed on the security container and must be completed and secured to the inside of the locking drawer of the security container or the vault door. The OF-89 is maintained by the custodian for the life of the security container. OF-89 is available in the GSA Forms Library website at https://www.gsa.gov/reference/forms/maintenance-record-for-security-containersvault-doors.

8. DFS will designate, for all departments responsible for a security container with classified holdings, at least 1 day a year when specific attention and effort is focused on disposing of unneeded classified material (clean-out-day).

9. Each GSA-approved security container that is in use must have a DFS-approved security plan that is stored inside the security container, regardless of the classification level of information within the security container.

10. The following are procedures for requesting a GSA-approved security container, changing a security container combination, transferring the security container to a new owner, relocating the security container, removing a security container from use, and reporting an unsecured security container.

(a) Requesting a GSA-Approved Security Container

NRC staff should create a ticket request through the NRC Service Catalog and complete the required information. A DFS staff member will then contact the requester regarding the security container. In an NRC regional location, staff should contact the security advisor and follow local office procedures. NRC Service Catalog is available at https://nuclepedia.usalearning.gov/index.php/Category:NRC_Service_Catalog.

(b) Changing a Security Container's Combination

The security container custodian will request a change in the security container's combination, if any of the following conditions exist:

(i) A new security 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 security container combination has been compromised or there is a possibility it has been compromised (i.e., unauthorized disclosure of the combination is suspected/the security container was left open),

(iv) The security container is no longer needed,

(v) The security container is found damaged, or

(vi) Once every year, in the absence of one of the conditions specified above.

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

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

(ii) The current owner's appointed security container custodian must work with their management to determine who will be designated as the new custodian of the security container. Once a new security container custodian has been determined and has been appointed in writing as a primary and alternate security container custodian; those individuals become responsible for any of the security container's existing and new contents. Ensure that the OF-89 is kept in the security container with the transfer of custody. The individuals must read and sign the security 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 security container is transferred shall result in a security incident, infraction, or violation.

(d) Relocating a Security Container

The security container custodian must complete an NRC Form 30 (NRCHQ), "Request for Administrative Services," and submit it to Facilities and Logistics Branch (FLB), DFS, ADM, with a copy to, and the regional security advisor, if FacilitiesSecurity.Resource@nrc.gov, KeysandLocks.Resource@nrc.gov, as appropriate. The form must contain information regarding the current location of the security container, its security container number (located on a plaque above the lock), and the location to where it will be moved. NRC Form 30 is available in the NRC Forms Library at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

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

(i) If a security container is being removed from active use, the security container custodian must ensure that all contents are properly destroyed or transferred, and that the security container is completely empty of all material except the OF 89. The security container custodian must then coordinate with DFS to get the combination reset and verify the security container is empty. After the combination has been reset, the security container custodian must complete an NRC Form 30 to remove the security container from use. Before submitting the NRC Form 30, DFS must reset the combination to the factory setting 50-25-50. Failure to do so may result in the security container not being removed.

(ii) REMINDER: If you have black label security containers, please contact DFS to have them replaced (they are being phased out of service). Below is the list of the GSA safes that are being phased out.

GSA CLASS	FED SPEC	REVISION
1	AA-F-357	A-F
2	AA-F-357	A-F
3	AA-F-358	A-F
4	AA-F-358	A-F
5	AA-F-358	A-F
5	AA-F-363	A-B
5	AA-D-600	A-B

GSA CLASS	FED SPEC	REVISION
6	AA-D-600	A-C
6	AA-F-358	A-F

(f) Reporting an Unsecured Security Container

The security container custodian must complete an NRC Form 183, "Report of Security Incident," if they find the security container unsecured. The security container custodian must immediately conduct an inventory of all items and submit written verification of all items' accountability. An NRC staff member, even if not the security container custodian, upon discovering the security container unsecured, will immediately contact the CAS and will stay with the security container until a PSO or a member of DFS arrives. Then, the reporting staff member should complete an NRC Form 183, no later than the next business day. NRC Form 183 is available in the NRC Forms Library at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

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

1. Introduction

(a) This section provides the practices and procedures for the protection of classified information in accordance with the AEA of 1954, as amended; the Energy Reorganization Act of 1974, as amended; pertinent E.O.s (e.g., E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," and E.O. 12968, "Access to Classified Information," 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. At the NRC, 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 (S), or Confidential (C); 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 required for access to specific classified information to perform or assist in a lawful and authorized Government function (E.O. 13526).

   (c) A person without appropriate access authorization for the area visited or the information contained in that area always must be escorted 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

   When not in use, all classified information up to and including Secret-RD must be stored in a GSA-approved security container (safe) 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) Classified reproduction shall be conducted only by authorized individuals who have the proper training and knowledge of the procedures for classified reproduction and only on DFS-approved, classified copy machines and in DFS-approved spaces. Copies of any classified information shall be protected using the same controls as the original version.

6. See MD 12.2, “NRC Classified Information Security 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 Top Secret and Secret-RD that DFS must review, label, and approve any cleared receptacles for them to be used for destruction of sensitive and/or classified information.

All categories of Sensitive Unclassified Non-Safeguards Information (SUNSI) (and CUI) can be destroyed by using a shred bin or by any means approved by the Office of the Chief Information Officer (OCIO) for the CUI program. When a shred bin is full and needs to be emptied, staff should call the CAS and provide the shred 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 shred 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 to be approved for such use. TS and Sensitive Compartmented Information (SCI) 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 the Security Management and Operations Branch (SMOB), DFS, and shall not be disposed of in shredders or shred bins, unless DFS provides 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, see MD 12.5, "NRC Cybersecurity Program."

(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 the AROs (see Section II.D of this handbook) 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.
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.

MI. Signage Posting Requirements

1. Facilities or real property, subject to the jurisdiction, administration, or in the custody of NRC, as per CFR 10 and Part 160, Section 229 of the Atomic Energy Act (AEA) of 1954, as amended, shall has signage identifying "Trespassing on Commission or Federal Property," 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 statutes contain a section regarding penalties for these actions. Trespassing on Commission or federal property can be considered a Class C felony. The types of posted signage identified and adherent to the Atomic Energy Act of 1954 are as follows:

(a) No Trespassing.

(b) Prohibited Articles.

(c) Area Under Surveillance.

2. Signage dimensions and color:

(a) “No Trespassing” signs must measure at a minimum 18 inches tall spaced 30 feet apart and 5 feet from the ground. The background must be white, have a red, white, and blue shield with black lettering in the center and white lettering in red and blue sections.

(b) “Prohibited Article” signs must measure at a minimum 10.5 inches by 13.5 inches. The background must be white with black lettering.

3. Leased Buildings

Signs must measure at a minimum 10.5 inches by 13.5 inches. The background must be white with black lettering.

4. Property Line (Owned/Leased)

Signs must measure at a minimum 10.5 inches by 13.5 inches. The background must be white with black lettering.

5. Controlled Area or Space

Contact DFS\SMOB for further information.

III. SECURITY ASSESSMENTS AND SURVEYS

A. NRC Facilities

DFS conducts security reviews, Physical Security Annual Assessment (PSAA) and Technical Security Countermeasure (TSCM) assessments of all NRC facilities in accordance with the latest Department of Homeland Security ISC Standards.

B. Secure Rooms

1. All new secure rooms within the NRC are constructed to meet the ICD-ICS 705, ICS 705-1, 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 Top-Secret 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, and its own access list that is updated, at minimum, annually by the ARO. Only those who have the proper clearance, have read and signed the security plan, and who are on the access list are allowed unescorted access into the room. All requirements within the room's security plan must be followed. Failure to follow the proper procedures shall be reported immediately to DFS and may result in a security incident, infraction, or violation.
2. All secure rooms must have, annually, a documented PSAA/TCSM assessment.
   (a) DFS will conduct the PSAA /TCSM assessments annually for secure rooms at NRC headquarters.
   (b) NRC regional locations will have annual PSAA/TSCM 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 the hosting NRC staff member, and present valid picture identification to enter any NRC facility. International visitors must follow the guidelines outlined in Section XV.C.
2. NRC staff members who will be hosting 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 host for the visitor must enter them 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 in the VARS entry. Vehicle information should be provided, if known.
3. The appropriate country code must be selected in VARS for an international visitor. The United States shall not be selected as the country of origin for any international visitor. If the international visitor has a visa, it must be presented along with their passport upon entry. For more information regarding international visitors, 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, Chair'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 at the discretion of DFS. VARS entries, screening, and visitor badging are still required.

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 name and phone number, and clearance level. This badge always must be worn prominently 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 badged contractor. An escort is not required when in an area designated as publicly accessible. An escort must adhere to all established escort policies.

G. International Visitors

If the international visitor has a visa in addition to a passport, the NRC POC must send a copy of both documents to InternationalVisitor.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 visiting any NRC facility. Additionally, the NRC POC must, before the international visitor's arrival, register them in VARS with the appropriate country code. See Section XIV.D of this handbook for more information about preparing for a visit from an international visitor.

H. Classified Visits

The process for organizing classified meetings and passing clearances are outlined in MD 12.2, Handbook, Section II.E, "Classified Conferences."

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 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) 201-3 (series) 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 wear their badge prominently ***above the waist***, so it is always visible while in NRC-controlled space and keep their badge in a compliant badge holder.
2. It is each cardholder's responsibility to maintain control of their 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 of NRC-controlled areas (e.g., off campus, outside NRC buildings, hanging/laying in a vehicle, any place not on NRC property and seen by public), a badged individual is required to conceal their badge and ensure it is physically protected.
4. A PIV card shall not be copied, replicated, or photographed for any purpose.
5. All cardholders must read and sign the "Privacy Act Statement Issuance of NRC Personal Identity Verification Card," agreement upon issuance.
6. 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 the same day, before they leave the facility.

D. Courier Cards

Any NRC staff member requesting a courier card 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 transported in a proper container after it has been properly packaged to ensure that it conceals any visual markings as described in MD 12.2. 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. NRC Form 90 is available in the NRC Forms Library in SharePoint at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

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 their termination or severance and notify DFS of the separation. Additionally, the COR must notify DFS if they are 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 SF-312, "Classified Information Nondisclosure Agreement (NDA)," 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 877, "Request for Security Support," 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, and it is the responsibility of the host office and not the PSOs 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. Controlled Unclassified Information or Safeguards Information Meetings

   (a) Public meetings or hearings involving subject matter categorized as restricted CUI, formally known as SUNSI or SGI. must be coordinated with DFS in advance to ensure that appropriate security measures are in place. An NRC Form 877 is required; however, no restricted CUI should be included or contained in the form.

   (b) All attendees in a CUI meeting must have their access authorization verified by the entity that granted their access to CUI. 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 277, "Request for Visit," 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. NRC Form 277 is available in the NRC Forms Library in SharePoint at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx

   (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 877. 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 to facilitate coordination with local law enforcement.

VII. SECURITY AWARENESS

A. Security Debriefings for Headquarters Exiting Employees

1. An NRC employee or temporary NRC employee (with a clearance) who is leaving the NRC must complete a security debriefing with DFS, SMOB, before their last day and surrender their NRC-issued PIV card before exiting the facility. This briefing is conducted using MS Teams and should be scheduled at least 1 week before the employee's departure from the NRC. If exigent circumstances exist, DFS should be contacted as soon as possible to coordinate alternative procedures.
2. The employee contacts DFS, SMOB, requesting a security debriefing before the last week of employment. SMOB normally conducts security exit briefings Monday through Friday, 7:00 a.m.-12 noon.
3. During the meeting, SMOB conducts the employee a security debriefing and directs the employee what section of the NRC Form 176, "Security Acknowledgement," and the SF-312 needs to be completed.
4. Before exiting the NRC for the last time, employees are required to return their PIV badge at the badging office, located at OWFN 1-F09, and the Personal Evacuation Kit (PEK) at the workstation location. A SMOB employee will retrieve the PEK kit.
5. Employees not returning to the NRC headquarters will be provided the address to mail their PIV card and if mailing to headquarters the PIV badge needs to be cut in half before mailing.

B. Security Debriefings for Regional Employees

1. A regional NRC employee or temporary NRC employee (with a clearance) who is leaving the NRC, must complete a security debriefing with the NRC regional security advisor if applicable, on their last day and surrender their NRC-issued PIV card before exiting the facility. This briefing is conducted through MS Teams and should be scheduled at least 1 week before the employee's departure from the NRC unless exigent circumstances exist in which case DFS, SMOB, 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 176, "Security Acknowledgment Statement" (available in the NRC Forms Library at https://usnrc.sharepoint.com/teams/NRC-Forms-Library/SitePages/Home.aspx.

C. 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) Enrolling, activating, terminating, and collecting PIV cards;
   (b) Administering the key and lock program for their region;
   (c) Serving as liaison with the FPS;
   (d) Serving as physical access control system administrator;
   (e) Serving as liaison with DFS for security incidents, security system concerns, issues, and/or repairs; and
   (f) Assisting with other security-related efforts at the direction of DFS.

VIII. SECURITY INCIDENTS, INFRACTIONS, AND VIOLATIONS

A. 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 CUI designated documents or material unattended, unsecured, or improperly stored;
3. Improper transmission of CUI designated documents or material;
4. Allowing an unauthorized person access to CUI designated 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.

B. 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. Failure to adhere to a DFS-approved security plan.

C. Security Violation

A security violation is an incident that could reasonably be expected to result in the actual or possible unauthorized disclosure of classified information covered under the requirements of E.O. 13526.

D. Reporting Security Incidents, Infractions, and Violations

1. NRC employees and contractors shall report all security incidents, infractions, and violations 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 https://usnrc.sharepoint.com/SitePages/Report-a-Safety-or-Security-Incident.aspx. For information regarding computer security incidents, please see MD 12.5.
2. A contractor shall immediately report all security incidents, infractions, and violations 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 the 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.

4. Classification of Reports

   Security incident reports shall be classified according to the content of the report and at the level prescribed by the applicable program security classification guides. At a minimum, reports shall be designated CUI to provide appropriate protection for information regarding personnel involved and information that could facilitate unauthorized access to classified information. If the lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered (e.g., media leak, public website posting, or loss in a foreign country), the report and location of the compromise (e.g., geographic location of unrecoverable material) shall be classified commensurate with the classification level of the compromised material to prevent further unauthorized disclosure.

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. Records

1. 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.
2. An agency head or senior agency official (or designee) 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), (3), and/or (4).

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, "Nuclear Regulatory Commission Insider Threat Program Policy Statement," (81 FR 9519) available at https://www.gpo.gov/fdsys/granule/FR-2016-02-25/2016-04026).

B. The ITP is led by ADM and supported by 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 their 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. INTERNATIONAL AND DOMESTIC TRAVEL THREAT RESPONSE PROCESS

The international threat response process is a process that advises agency management of safety, security, and threat-related information to make a risk-informed decision for NRC staff planning for or currently on official international 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, "International and Domestic Travel Threat Response Process" (ML16085A245), 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 international and domestic travel, and provides a recommendation to the EDO to make a risk-informed decision regarding official agency staff travel.

B. Unofficial Foreign Travel: All NRC covered individuals (clearance holders) are required to report and gain agency approval for all unofficial (personal) foreign travel using the Security Executive Agent Directive 3 (SEAD3) portal as set forth by the Director of National Intelligence (ODNI), signed on December 14, 2016. All NRC covered individuals must enroll in the Department of State's Smart Travel Enrollment Program (STEP) before travel. Both actions must be completed no later than 5 days before travel.

XII. PROHIBITIONS ON WIRETAPPING AND EAVESDROPPING DEVICES

A. Introduction

Surreptitious use of wiretapping or eavesdropping devices in conversations or wire transmission (including wireless) without the consent of all the participants are strictly prohibited.

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 NRC facilities. The OEP applies to all building occupants, including employees, contractors, and visitors, and 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. The OEP shall be reviewed annually for any necessary updates.

B. Personal Evacuation Kits (PEKs)

PEKs are available to all NRC employees and 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. For those who work or maybe working at headquarters for an extended amount of time; PEKs, and the items contained within them, can be located in the headquarters supply room located at OWFN-P1-C12.

XIV. INTERNATIONAL PROGRAMS

A. Introduction

All international visitors who come to an NRC facility shall be considered, without exception, an international assignee, a trainee, or a visitor. The following section describes DFS's role in the various international programs.

B. International Assignee Program

1. An international assignee is an individual from an international regulatory authority who is sponsored by either their country or the International Atomic Energy Agency (IAEA) and assigned to the NRC for an extended time, consistent with applicable policies and other formal agreements. For information regarding international assignees, see MD 5.13, "NRC International Activities, Practices, and Procedures."

2. DFS\SMOB reviews, evaluates, and approves the international 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 international assignee. DFS must be notified of any change to the international 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 international assignee is approved for access to CUI, 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 CUI. Failure to comply with, or any unauthorized deviation from, the international 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 international assignee a badge upon arrival. The assignee must return their 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. International Trainee Program

1. In order for an international trainee to register and attend an NRC-sponsored training either in person at the Technical Training Center (TTC) or virtually (online), the OIP International Training Program Manager (ITPM) will send DFS, the completed NRC Form 121, "Request for Non-Virtual Training for International Trainees," and the NRC Form 70A, "Request for Name Check," to InternationalTrainee.Resource@nrc.gov for each requestor and include an electronic copy of the requestor's passport and visa, if the international trainee has a visa in addition to a passport. In addition, OIP should confirm its understanding that name check requests must be submitted at least 20 business days before the start date (if applicable) of the course. DFS will conduct background checks for all international trainees attending NRC training in person and virtually (online).

2. Upon receipt of results from the NRC Form 70A, DFS will review the NRC Form 121, and make a determination. Once approved, DFS will send copies of the NRC Form 121 to the appropriate parties identified on the form. If results are not received before the start of training, DFS will coordinate with OIP to determine how to proceed.

3. For detailed information regarding international trainees attending NRC-sponsored training, see MD 5.13.

D. International Visitor

1. Before an international visitor arrives for their visit, the NRC host for the visitor shall 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 international visitor 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 password protected copy of the passport and visa to InternationalVisitor.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 during the visit (e.g., publicly available, CUI, SGI, and/or classified);

      (v) The OIP desk officer informed of the visit; and

      (vi) If needed, request for security support.

2. The international visitor will be screened through security and provided a visitor badge upon entering the building and always must be escorted in NRC-controlled space. Additionally, the international 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. ASSIGNMENT OF INTERNATIONAL REGULATORY EMPLOYEES TO THE NRC

A. Introduction

Guidelines are given for the prevention of unauthorized access to classified information or sensitive unclassified information by international regulatory employees assigned to the NRC. The responsibilities of OIP; ADM, DFS; supervisors; and employees are outlined below.

B. Activity Plans

OIP, in cooperation with DFS, will establish and coordinate the assignee program and individual assignee activity plans that enumerate the variety of activities in which the assignee is authorized to participate.

C. Assignment

Information about assignments for international visitors can be found in MD 5.13, “NRC International Activities, Practices, and Procedures,” Handbook Section VII.B, “Foreign Assignee.”

D. Background Check

Before inviting the international regulatory employee to join the NRC, OIP will obtain the required background and biographical data and submit the data to SMOB with a request that the appropriate indices checks be conducted by the appropriate Federal agencies. Information that creates a question as to whether assignment of the international regulatory employee is consistent with national interest will be evaluated by SMOB and forwarded with a recommendation to OIP.

E. International Assignee Agreements

International assignees will be required to sign a commitment patterned after the agreement signed by Government contract consultants agreeing not to take any proprietary documents away from their proper place of use and storage and not to disclose proprietary information or otherwise violate the conditions under which NRC employees receive and use this information. The signing of the confidentiality agreement by the assignee is a condition of the assignment in accordance with the terms of the agency-to-agency agreement that both the NRC and the international regulatory agency sign. Specific procedures are as follows:

1. The supervisor of an assignee will determine if an assignee needs to have access to proprietary information. A separate determination of need will be made for the proprietary information related to each program area in which the assignee is authorized to work. The supervisor will prepare a note concerning this access and will maintain a listing of documents to which the assignee has access. Whenever work on a program area is terminated, and at the end of each assignment, the assignee will return all proprietary documents. The supervisor of the assignee will ensure that all documents on the assignee's list are returned.
2. Access to special classes of information, including details of facility security plans, material control and accounting information, and SGI that is subject to 10 CFR 73.21 must not be granted unless approved by NSIR.

F. Security Plans

1. Before the invitation letter is issued, representatives from DFS, OIP, and the office to which the international employee will be assigned will work together to define the assignment and to develop a security plan for each assignee. The host office will be responsible for developing the plan. This plan must be developed and approved before the assignee arrives. Each international assignee will be required to read, agree to, and sign the security plan. The plan will require the approval of OIP, the host office, and DFS, and must include the following elements:

   (a) Description of the physical location of the assignment within NRC, a licensee facility, or another facility.

   (b) Identification of specific areas to which the assignee is to be given unescorted access to perform essential responsibilities. (The assignee's access should be consistent with the requirements of DFS and the assignments of the host office.)

   (c) Explanation of special badging required and associated restrictions.

   (d) Explanation of restrictions on the use of, or connection to, NRC computing resources such as LANs, other NRC computing systems, document management systems, and sensitive data.

   (e) Discussion of the ways in which commercial or foreign proprietary information must be protected if the assignment requires access to this information. (Assignments should normally be tailored so that they do not require access to this information.)

   (f) Instructions on alerting co-workers about an assignee's presence and the assignee's restricted access, both physical and informational, including a DFS counterintelligence-type briefing.

   (g) Assignment of a supervisor and an alternate to monitor the assignee's day-to-day activities.

   (h) Requirement for monthly or quarterly progress reports from the assignee. (Copies of the report are to be sent to the supervisor and other appropriate persons in the office to which the international assignee is assigned.)

   (i) Requirement for a mid-point (or more frequent) interview by DFS of the assignee, the assignee's supervisors, and, as appropriate, the assignee's co-workers to ensure that the assignee and supervisors are continuing to comply with the approved security plan. (Any problems will be reported to OIP and any other appropriate office.)

2. If later experience indicates that the security plan requirements cannot be met, or conditions change that warrant a possible change in requirements, or if any other problems arise, the supervisor will immediately advise OIP and DFS. Any changes in the security plan must be approved by DFS and OIP.

3. DFS will issue assignees special identification badges. These badges, while allowing assignees unescorted access to specific areas, are prominently marked “Assignee” and are color-coded red for “no access.” International assignees will be required to always wear their badges.
4. Co-workers and other NRC employees in the assignee's area also will be made aware of the requirement for the assignee to always wear the badge. Access by the assignee into areas not specified in the plan will require that the assignee be escorted by a cleared NRC employee designated by the assignee's supervisor.
5. The assignee's supervisor will make an initial evaluation of an assignee's work area, as well as a revaluation at the midpoint of the assignment and at any time the security plan is amended. Any recommendations should be given to DFS for action at this time.

G. Assignee Responsibilities

1. Assignees will not authorize visits by other individuals to the NRC, NRC contractors, or other NRC facilities.
2. Assignee duties are to be limited to those that do not require representing the NRC in public or acting as an official representative in meetings with NRC licensees.
3. Assignees will be responsible for obtaining and making whatever copies of records or documents they wish to take with them before completion of their assignments. Assignees will be required to obtain the supervisor's approval before copying these records and will also be required to provide a list of these records to their NRC supervisors, OIP, and DFS.

H. Evaluation of Assignees

Upon completion of the assignment, OIP will provide an evaluation form to the supervisor. The supervisor will complete the form and send copies to OIP, DFS, and the cognizant office director or regional administrator.

XVI. INDUSTRIAL SECURITY PROGRAM

A. Introduction

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) (32 CFR Part 117) 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 32 CFR Part 117, 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.”

B. Cognizant Security Authority (CSA)

1. As a CSA, the NRC is required to grant FCLs and provide oversight and assistance for 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.

2. 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, 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 32 CFR 117, “National Industrial Security Program Operating Manual (NISPOM).”

3. 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 their records.

C. Facility Security Clearances

1. FCL with Reciprocity - Multiple CSAs

   (a) If 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) If 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 the NRC or another CSA would give under the requirements of the NISP. The CSAs will work together to determine who will be the lead CSA for the contractor.

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

   (a) If 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 to determine if the contractor is eligible for an FCL. Upon completion of the survey process, DFS will decide 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.

D. Foreign Ownership, Control, or Influence (FOCI) Approval and Reviews

1. As established earlier in this section, the FCL approval process is an in-depth review of an entity’s ability to access and protect classified information. During the FCL review process, a FOCI determination is made. A FOCI determination is defined in the National Industrial Security Program Operating Manual (NISPOM) as follows:

   “A U.S. company is considered to be under FOCI when a foreign interest has power, direct or indirect, whether or not exercised, to direct or decide matters affecting the management or operations of the company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.”

2. A company under FOCI is not eligible for an FCL. However, a company may be granted an FCL if the risk of the foreign ownership, control, or influence can be mitigated in conformity with the national interest. This is referred to as FOCI Mitigation, a process whereby unauthorized access to classified information is prevented. FOCI Mitigation uses various security measures, safeguards, and restrictions to prevent unauthorized access.

3. There are seven factors by which the nature and extent of FOCI are analyzed. Each one of these factors examines the nature of the situation surrounding FOCI. The factors are then analyzed in the aggregate to determine the level of mitigation

required. However, before they can be analyzed, they must be identified accurately, and understood within the context of the organization's need for an FCL.

4. The FOCI factors that must be identified are—

   (a) Any record of economic and Government espionage against U.S. targets;

   (b) Any record of engagement in unauthorized technology transfer, including being the target of enforcement;

   (c) The type and sensitivity of information requiring protection;

   (d) The source, nature, and extent of the FOCI;

   (e) Any record of compliance with U.S. laws, regulations, and contracts;

   (f) The nature of bilateral and multilateral security and information exchange; and

   (g) Ownership or control, in whole or in part, by a foreign government.

E. Recurring Requirements for FCL Holders

1. Annual reviews are required for all entities with an FCL issued by the NRC, or through the reciprocity process, a FOCI mitigation, companies with parent organizations excluded by formal resolution or organizations that have filed board resolutions to reduce non-controlling foreign ownership.

2. Facility clearance requirements state that procedures must be in place to verify changes in Key Management Personnel (KMPs), and to ensure that all KMPs are processed for and granted access authorizations.

3. All FCL holders who are contracted to the NRC are subject to random reviews throughout the duration of their facility clearance with NRC HQ. Companies are notified 30 days in advance of the review.

F. Facility Security Clearance Oversight

1. Contractor reviews: Security Vulnerability Assessments (SVAs)

   (a) DFS conducts onsite security vulnerability assessments (SVAs) of each contractor awarded an FCL for work on an NRC classified contract every 2 years. In accordance with 32 CFR 117, contractors review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles. Contractors with non-possessing FCLs (no classified storage at the contractor’s location) will be assessed approximately every 2 years. Any FCL review time starts from the date the FCL was first issued. The review cycle scope and frequency may increase or decrease consistent with risk management principles.

(b) There are four types of SVAs:

(i) Self-inspection: The contractors review their security programs on a continuing basis and conduct a formal self-inspection at least **annually** and at intervals consistent with risk management principles.

(ii) Compliance (Oversight Reviews) SVA: DFS will conduct a formal Oversight Review SVA every **2 years** or at their discretion and is subject to change. A second type of compliance SVA is if a regularly scheduled compliance SVA has an Unsatisfactory assessment, then a second compliance SVA will be scheduled to ensure that the issue has been brought to compliance.

(iii) Unannounced SVA: Can be conducted at any time with little to no notice.

(iv) Closeout SVA: A closeout SVA is conducted when a possessing contractor is terminated, regardless of the reason for termination, to ensure all classified material is returned to the NRC or accounted for before terminating the FCL.

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

(d) 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 because 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.

G. 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 is not 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 is mailed to the contractor as confirmation, and the contractor’s file folder is maintained for a minimum of 2 years in the event the contractor re-enters the NISP.

5. Termination of Contractor Employee Access Authorizations

   A contractor employee who no longer requires NRC access authorization due to termination of an FCL, will be removed from access and properly debriefed.

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.

If more than 4 individuals require the combination to the security container, annotate their information on a separate blank sheet of paper and include it with the SF 700 in the opaque envelope marked security container in accordance with Section II.J.4 of this directive.

Exhibit 2 Optional Form 89, "Maintenance Record for Security Containers/Vault Doors"

MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS

NOTE: Store this form in the security container or on the vault door.

TYPE ☐ SECURITY CONTAINER ☐ VAULT DOOR

SERIAL NUMBER (Containers: Located on the side of the control drawer. Vault Doors and Map and Plan Containers: Located on the inside face of the door.)

MANUFACTURER

GSA CLASS ☐ ONE ☐ TWO ☐ THREE ☐ FOUR ☐ FIVE ☐ SIX ☐ SEVEN

OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION

OPTIONAL FORM 89 (9-98)

OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED

OPTIONAL FORM 89 (9-98) BACK