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

MD 12.1	NRC FACILITY SECURITY PROGRAM	DT-11-12
Volume 12:	Security	
Approved By:	R. William Borchardt Executive Director for Operations	
Date Approved:	September 14, 2011	
Expiration Date:	September 14, 2016	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Darlene Fenton 301-415-7050	

EXECUTIVE SUMMARY

Directive and Handbook 12.1, "NRC Facility Security Program," are being revised to incorporate a recommended change in the handbook resulting from OIG Audit 08-A-10 regarding annual physical security inspections of Continuity of Operations Centers.

TABLE OF CONTENTS

I. POLICY

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

II. OBJECTIVES

- Ensure that classified and sensitive unclassified information is protected from unauthorized disclosure under pertinent laws, Executive Orders, management directives, and applicable directives of other Federal agencies and organizations.
- Ensure that assets in NRC facilities are protected from harm, damage, loss, or misuse to the greatest extent possible.
- Ensure the administration of the NRC Security Education/Awareness Program and the NRC Security Infraction Program.
- Ensure the limitation on wiretapping and eavesdropping devices in NRC facilities.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Executive Director for Operations (EDO)

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

B. Inspector General (IG)

1. Provides the Division of Facilities and Security (DFS), Office of Administration (ADM), when appropriate, any information developed or received relating to security 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 security guards, 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.

Office of the Inspector General GG-1811 series criminal investigators may be called upon to assist and are authorized by statute to carry a firearm, to make an arrest without a warrant, and to seek and execute warrants for arrest, search of premises, or seizure of evidence.

4. Approves in accordance with Department of Justice (DOJ) guidance the surreptitious use of electronic, mechanical, or other devices for monitoring, recording, or intercepting conversations, as authorized by law.

C. Deputy Executive Director for Corporate Management (DEDCM)

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, the adequacy of security protections for NRC automated information systems and for the information contained in those systems.

D. General Counsel (GC)

Performs legal review of facility security-related matters and concurs in the Executive Director for Operations decision to authorize and conduct any monitoring or recording of conversations.

E. Director, Office of International Programs (OIP)

Provides the required information for the security assessment, upon request, through appropriate intergovernmental liaison channels.

F. Director, Office of Administration (ADM)

Develops overall policy and oversees the NRC Facility Security Program and Occupant Emergency Program (OEP) as carried out by DFS.

G. 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, the intelligence and law enforcement communities, the Department of Energy, 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, inspections, and security education/awareness activities. Administers the NRC

counterintelligence, secure telecommunications, foreign disclosure of information, and authorized classifier programs.

4. Acts as the NRC Central Office of Record for Communications Security (COMSEC) and operates the NRC's secure communications.

5. Develops, maintains, and integrates NRC plans, procedures, and training for response to domestic and international radiological events and to any incidents that threaten the Continuity of Government (COG) or the NRC Continuity of Operations (COOP).

H. Director, Office of Information Services (OIS)

Administers the information security programs that deal with sensitive unclassified information through guidance, oversight, inspections, and security education/awareness activities.

I. Director, Office of Investigations (OI)

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

2. Authorizes carrying of firearms by Office of Investigations (OI) criminal investigators (special agents). If designated and sworn as Special Deputy United States Marshals, OI special agents are authorized to carry firearms in accordance with agency policy while in the performance of official duties.

J. Office Directors and Regional Administrators

1. Ensure that NRC employees and NRC contractor personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook, as appropriate.

2. Advise DFS, ADM, of the existence or proposed creation of any business relationship or interest that would require DFS review of any contract, subcontract, or similar action and of any significant change or termination of any classified or sensitive unclassified interests in organizations and functions under their jurisdiction.

3. Submit facility physical security plans to DFS, from their respective office or region, for review and approval, include location, purpose/nature of activity, classification level, access list, point of contacts, equipment needed, hardware/software to be used, operating procedures, hours of operation, contingency plan, maintenance procedures, etc.

4. Advise DFS, ADM; the Office of Nuclear Security and Incident Response (NSIR); or the Office of Information Services (OIS) in their areas of responsibility, of any information that indicates noncompliance with this directive and handbook or that is otherwise pertinent to the proper protection of classified information, sensitive unclassified information, or NRC assets.

5. Take or direct action, as requested by DFS, or as otherwise may be pertinent, regarding deficiencies in security or property protection in facilities or functions under their jurisdiction.
6. Support and implement the NRC Security Education/Awareness Program for personnel under their jurisdiction, including ensuring that subordinate NRC supervisors discharge their responsibility for on-the-job security education and awareness of their employees.
7. Support and implement the NRC Security Infraction Program in all organizations and functions under their jurisdiction, including submitting infraction reports to DFS.
8. Control and safeguard classified and sensitive unclassified information under their jurisdiction in accordance with this directive and handbook.
9. Make written requests to the Director of DFS, ADM; Director of NSIR; or Director of OIS for exceptions to their respective requirements or deviations from this directive and handbook.

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

1. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC Facility Security Program, including the approval of facilities for the handling and storage of classified and sensitive unclassified information.
2. Administers the NRC Security Education/Awareness Program for physical and personnel security matters.
3. Administers the NRC Security Infraction 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 the Office of the Inspector General of law enforcement, employee misconduct, and contractor wrongdoing matters, as appropriate.

IV. APPLICABILITY

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

V. DIRECTIVE HANDBOOK

Handbook 12.1 contains guidelines and procedures with regard to facility security, the protection of classified information and facilities, the safeguarding of NRC property and programs, the administration of the NRC Security Education/Awareness Program and the Security Infraction Program, and limitations on wiretapping and eavesdropping devices.

VI. REFERENCES

Code of Federal Regulations

10 CFR Part 25, "Access Authorization."

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

10 CFR Part 160, "Trespassing on Commission Property."

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

Department of Defense

National Industrial Security Program Operating Manual (NISPOM), Department of Defense 5220.22M, February 28, 2006, and Supplement 1, April 1, 2004.

Department of Justice

Department of Justice's (DOJ's) Vulnerability Assessment of Federal Facilities, June 28, 1995.

Director of Central Intelligence Directives

Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," November 18, 2002.

Executive Orders

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

E.O. 12829, "National Industrial Security Program" (NISP), January 6, 1993.

E.O. 12958, as amended, "Classified National Security Information," April 17, 1995.

E.O. 13142, "Amendment to Executive Order 12958 - Classified National Security," November 19, 1999.

E.O. 13292, "Further Amendment to Executive Order 12958, As Amended, Classified National Security Information," March 25, 2003.

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

Interagency Security Committee

Interagency Security Committee (ISC) Security Criteria for New Federal Office Buildings and Major Modernization Projects.

Intelligence Community

Intelligence Community Standard No. 705-1, "Physical and Technical Security Standards for Sensitive Compartmentalized Information Faculties."

National Security Agency

National Security Agency (NSA) performance requirements for High Security Crosscut Paper Shredders - NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders.

NACSI 4005, "Standard Criteria for Safeguarding Communications Security Material," August 22, 1973.

National Institute of Standards and Technology

FIPS PUB 201-1, Federal Information Processing Standards Publication, "Personal Identity Verification (PIV) of Federal Employees and Contractors."

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."

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)."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.5, "NRC Automated Information Security Program."

NRC, OIG, "Special Agents Handbook."

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

Occupant Emergency Plan Web Site for NRC Headquarters and the Regional Offices: http://www.internal.nrc.gov/security.html.

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.

Security Policy Board, Executive Branch

Provisions of the NISP, September 19, 1996.

Underwriters Lab

Underwriters Laboratory (UL) Standard 2050.

United States Code

Americans With Disabilities Act of 1990 (ADA) (42 U.S.C. 12101 et seq.).

Atomic Energy Act 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 (Title 18 of the *United States Code*).

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).

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-11-12
Volume 12:	Security	
Approved By:	R. William Borchardt Executive Director for Operations	
Date Approved:	September 14, 2011	
Expiration Date:	September 14, 2016	
Issuing Office:	Office of Administration Division of Facilities and Security	
Contact Name:	Darlene Fenton 301-415-7050	

EXECUTIVE SUMMARY

Directive and Handbook 12.1, "NRC Facility Security Program," are being revised to incorporate a recommended change, in the handbook, resulting from OIG Audit 08-A-10 regarding conducting annual physical security inspections of Continuity of Operations Centers.

TABLE OF CONTENTS

EXHIBITS

I. FACILITY CLEARANCE AND SURVEYS

A. Introduction

Section I provides procedures for granting and terminating NRC clearances for security facilities, designating and terminating physical protection facilities, and surveying these facilities to ensure compliance with established security standards.

B. Establishment of Security Facilities

1. Basic Considerations

(a) A security facility is any facility that has been cleared by NRC to use, process, store, reproduce, transmit, or otherwise handle NRC classified information. Security facilities are established to provide a standardized program of protection for classified information at the locations involved.

(b) Facility clearance is the process by which NRC determines that a facility is eligible to handle NRC classified information. The Division of Facilities and Security (DFS), Office of Administration (ADM), surveys these facilities to evaluate the adequacy of the security protection afforded NRC classified information. NRC facility clearance is granted at a level commensurate with the anticipated level of NRC classified information to be received, stored, or otherwise handled by the facility.

(c) In certain instances, DFS bases facility clearance on assurances from another Federal agency that has similar security measures in place. In these instances, the facility must be under the active direction of that agency's security program, and DFS must be provided written assurance that NRC classified information will be afforded protection in accordance with acceptable security criteria, such as Executive Order 12958, "Classified National Security Information," and other applicable national security guidance.

2. Notification of Classified Interests

   (a) All NRC offices and divisions must promptly notify DFS of their intent to initiate any classified contract, subcontract, or similar interest under their jurisdiction or sponsorship. A completed NRC Form 187, “Contract Security and/or Classification Requirements,” and a statement of work must be submitted to DFS. On the basis of this submission, DFS will initiate necessary actions to confirm an existing facility security clearance or establish such a clearance for the facility.

   (b) An existing facility clearance may be used provided the approval for classified information is at the same or lower classification level as the proposed security interest. The responsible NRC office shall notify DFS or the Office of Nuclear Security and Incident Response (NSIR) (for licensees) of any significant change in or termination of a classified interest previously reported. Additional information and guidance concerning contract administration can be found in Management Directive (MD) 11.1, “NRC Acquisition of Supplies and Services.”

C. The Facility Clearance Process

1. NRC, NRC Contractor, and NRC Consultant Facilities

   (a) The basis for facility clearance is a favorable foreign ownership, control, or influence (FOCI) determination (reference MD 12.2, “NRC Classified Information Security Program,” Part I.F); a satisfactory security survey rating; an appropriate number of personnel access authorizations; and a DFS-approved facility security plan. The security plan must be prepared and the security survey must be conducted no more than 6 months before the facility clearance is granted. If more than 6 months has elapsed, DFS will conduct a special survey or otherwise ensure that the conditions and procedures described in the security survey report and the security plan are still in effect (reference 10 CFR Part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data”).

   (b) Although the nature of a security plan dictates that each plan be somewhat unique, all security plans must contain a written statement originated by the appropriate NRC office, division, region, contractor, consultant, or other interest describing the organization's procedures and measures for safeguarding NRC classified information and for ensuring that employees receive security education. As a rule, the requirements contained in this directive will be used in formulating the security plan. DFS may be consulted at any time for advice and assistance to develop the required security plan and normally provides this assistance as a matter of course during the facility clearance process.

(c) In special instances, DFS may grant an interim facility clearance before an initial security survey is conducted. Interim facility clearance will be granted based on a favorable FOCI determination, an appropriate number of NRC access authorizations, and a DFS-approved facility security plan. Thereafter, the initial security survey will be conducted as soon as practical. As a result of the initial security survey, DFS will grant facility clearance, will continue the interim facility clearance pending compliance with survey recommendations, or will deny facility clearance and terminate the interim facility clearance.

2. Special Requirements for the Department of Energy National Laboratories

Department of Energy (DOE) work performed for NRC is subject to security requirements other than the provisions of this section. These other requirements are contained in the National Industrial Security Program Operating Manual (NISPOM) dated January 1995, and Supplement 1 dated February 1995, or any succeeding NISPOM guidance. Under the NISPOM, DOE assumes security cognizance for NRC classified interests at DOE national laboratory facilities. All NRC offices and divisions must promptly notify DFS of their intent to initiate NRC classified work at DOE national laboratories. (See also MD 11.7, “NRC Procedures for Placement and Monitoring of Work With the U.S. Department of Energy (DOE).”)

3. Special Requirements for Industrial Facilities at Which NRC and DOE Have Interests

For industrial facilities, defined as non-Governmental organizations other than the national laboratories and the United States Enrichment Corporation, at which both NRC and DOE have authorized either the possession of or access to (nonpossessing facilities) classified information, security requirements other than the provisions of this section are specified in a DOE and NRC Memorandum of Understanding (MOU), dated September 19, 1996. Under this MOU, NRC and DOE agree to provide mutual security services for the protection of classified information released to or within industry on behalf of NRC using the specific requirements, restrictions, and other safeguards as prescribed in the NISPOM and its supplement.

4. Facilities of the Department of Defense (DOD), DOD Contractors, and DOD Consultants

(a) Under the National Industrial Security Program (NISP), DOD is responsible for the security, as prescribed in the NISPOM and its supplement, of all classified interests at its facilities; therefore, NRC facility clearance is not necessary.

(b) An MOU between NRC and DOD, dated April 2, 1996, reflects an agreement that NRC and DOE will provide mutual security services for the protection of classified information released to or within industry on behalf of NRC or DOD. The MOU further states that NRC and DOD will apply the specific requirements,

restrictions, and other safeguards as prescribed in the NISPOM and its supplement.

(c) Certain additional security considerations may be required in the following instances:

(i) Existing DOD Contractor and Consultant Facilities Engaged Directly by NRC or Its Contractors for Work Involving Classified Information

NRC approval to perform work requiring access to NRC classified information is based on the existing DOD facility clearance (Confidential, Secret, or Top Secret), provided that the DOD facility clearance includes the NRC classified interest. The responsible DOD security office shall furnish DFS a copy of its security inspection report covering, or otherwise ensuring, the adequate security protection of the NRC classified interest at the facility. The responsible DOD security office must agree that it will notify DFS before its facility clearance is downgraded or terminated. All DOD contractors and consultants having access to NRC classified information must hold comparable DOD access authorizations. If Restricted Data is involved, the mandatory personnel access authorization requirements of the Atomic Energy Act of 1954, as amended, must be followed (reference 10 CFR Part 95).

(ii) Special Considerations

If the requirements of Section I.C.4(c) of this handbook are not met, or if NRC Top Secret information is involved, DFS shall grant facility clearance in accordance with Section I.C.1 of this handbook.

5. Other Federal Agencies (Excluding DOD Facilities) and Their Contractors or Consultants

(a) An NRC facility clearance can be provided based on written assurance from a responsible official of another agency that NRC classified information in its possession or in the possession of its contractors and consultants will be provided appropriate protection. The responsible agency official will provide either a copy of the other agency's security inspection report or similar assurance that documents the adequate security protection of the NRC classified interests at the facility.

(b) If this assurance cannot be obtained, a facility clearance may be granted in accordance with the procedures contained in Section I.C.1 of this handbook. Additionally, if a specific agreement exists between NRC and another Federal agency that limits the dissemination of certain categories of NRC classified information within that agency, DFS will, upon execution of the agreement, request that agency to furnish a statement of its procedures for ensuring the

limitation. The responsible Federal agency security office must agree that it will notify DFS in writing before its facility clearance is downgraded or terminated.

D. Continuing Facility Clearance

At each security facility, DFS assesses compliance with security requirements and the adequacy of procedures to safeguard NRC classified information. This continuing assessment program for each type of facility includes the following:

1. NRC, NRC Contractor, and NRC Consultant Facilities

   Require a periodic security survey resulting in a “satisfactory” security rating.

2. DOE National Laboratories

   See Section I.C.2 of this handbook for special requirements.

3. DOD, DOD Contractor, and DOD Consultant Facilities

   (a) Generally, NRC periodic surveys are not required. However, if an agreement exists between NRC and DOD (or another Federal agency subject to DOD industrial security services) that specifically limits the dissemination of certain categories of NRC classified information, the responsible security official will submit an annual statement to DFS addressing the effectiveness of the other agency's procedures in meeting this agreement.

   (b) Other security measures may be required for existing DOD contractor and consultant facilities engaged directly by NRC or its contractors for work involving NRC classified information. These security measures require the responsible DOD security office to furnish DFS, on a periodic basis, a copy of its security inspection report, or other assurance of adequate security safeguards, covering the NRC Confidential or Secret interests at the facility.

4. Other Federal Agencies (Excluding DOD Facilities) and Their Contractors and Consultants

   Normally, periodic surveys are not required, except as specified in Section I.D.4(b) of this handbook. However, surveys may be conducted upon request by or agreement with the particular agency involved. Additionally, other security measures may be required in the following instances:

   (a) Special Considerations

   If an agreement exists between NRC and the Federal agency to limit the dissemination of certain categories of NRC classified information, the responsible Federal agency security office must submit an annual statement to DFS regarding the effectiveness of its procedures in meeting this agreement.

(b) Federal Records Centers

A periodic security survey resulting in a "satisfactory" security rating is required for a Federal Records Center (FRC) storing NRC classified information. (See Section II.H.3(c) of this handbook for more information on FRCs.)

E. Terminating Facility Clearance

1. DFS will terminate the facility clearance when a facility has completed its NRC classified activities or no longer requires NRC classified information. NRC sponsoring office shall notify DFS when a facility clearance termination is required. In these cases, DFS will ensure that classified information has been destroyed or returned to appropriate NRC custody.

2. In certain instances, the responsible party may demonstrate a need to retain possession of NRC classified information after the completion or termination of an NRC contract, subcontract, or other agreement. The responsible party shall complete a "Certificate of Possession" (see Exhibit 1), and DFS will conduct periodic security surveys to ensure the continued protection of NRC classified information.

3. However, when the termination of an NRC classified interest results in the termination of the facility clearance, this process is accomplished by means of a termination survey, by correspondence, or other appropriate means, and includes the actions described below:

(a) Security Termination Statements

All individuals granted NRC access authorizations who, as a result of the termination of the contract, subcontract, or other agreement, no longer require NRC access authorizations, shall complete and forward to DFS, through the responsible security official, an NRC Form 136, "Security Termination Statement."

(b) Certificate of Nonpossession

The responsible security official, or other designated official, shall complete and forward to DFS a "Certificate of Nonpossession" (Exhibit 2), which certifies that all NRC classified information associated with the contract, subcontract, or other agreement has been destroyed in accordance with NRC security regulations or has been returned to appropriate NRC custody.

(c) Cancellation of Pending Access Authorizations

The responsible Federal agency security office shall notify DFS in writing to cancel all pending requests for access authorization under the terminated contract, subcontract, or other agreement.

F. Special Considerations Applicable to Bidders

1. Facility clearances for bidders or prospective contractors are granted, continued, or terminated in accordance with Sections I.B through I.E of this handbook. These clearances may be granted on a short-term basis for a particular procurement action or continued on a standby status to accommodate a current or projected procurement action.

2. Unsuccessful bidders are required to destroy or return to NRC custody all classified information received or generated in connection with their proposals, as directed by the NRC official issuing the solicitation. This action must be accomplished within 15 days after receipt of notification that a purchase order or a contract has been awarded or that the bid invitation has been withdrawn.

G. Security Surveys

1. Types of Surveys

   A security survey of an NRC facility, internal organizational component, or an NRC contractor facility provides a basis for evaluating the adequacy and effectiveness of the administration of the security program and the protection afforded NRC classified or sensitive unclassified information, employees, and assets. It also thoroughly examines the policies and procedures in effect to ensure compliance with NRC security regulations. DFS will conduct these surveys which will include—

   (a) Initial Security Survey

   A survey conducted before a facility clearance is granted.

   (b) Periodic Security Survey

   A facility or organizational survey conducted at regular or scheduled intervals. The frequency is determined by the sensitivity, special circumstances, and local environment encompassing the facility. Continuity of Operations centers require, at a minimum, an annual physical security survey.

   (c) Special Security Survey

   A facility or organizational survey conducted to address specific or immediate problems, questions, or deficiencies.

   (d) Termination Security Survey

   A facility survey conducted to ensure the proper termination of NRC security interests.

2. Coverage

   (a) Initial and periodic security surveys examine safeguards afforded all NRC classified interests and include a critical examination of all applicable components and elements of the security program.

   (b) Special security surveys evaluate the adequacy of existing protection for new activities and the need for changes to security procedures as a result of other conditions, such as renovation or remodeling of the facility, or new security measures to correct security deficiencies.

   (c) Termination security surveys ensure classified interests are terminated and security termination actions are completed.

3. Reporting

   (a) Report of Survey

   Following the completion of a security or physical protection survey (see Section I.H of this handbook), DFS prepares a written report to document the results of the survey and verbally advises the responsible organization of all deficiencies and recommendations.

   (b) Report of Action Taken

   Upon receipt of DFS's survey findings, the responsible organization shall inform DFS of those actions taken by the date specified by DFS. When the required action cannot be completed by the prescribed date, the responsible organization will inform DFS of the status of the action to be taken.

   (c) Immediate Corrective Action

   When a security deficiency is discovered that poses an imminent or serious threat to NRC classified interests, DFS provides immediate onsite direction to correct the deficiency. When such a situation cannot be corrected, DFS takes immediate measures to remove the classified interests and suspend or terminate facility clearance pending corrective action. Similarly, the responsible organization or facility shall immediately notify DFS of any situation or occurrence that poses an imminent or serious threat to NRC classified interests. When appropriate, DFS will notify the Office of the Inspector General (OIG). DFS provides advice and assistance as to any corrective actions to be taken. Similarly, immediate actions will be taken, as appropriate, to address deficiencies that pose an imminent or serious threat to NRC sensitive unclassified interests. DFS will notify OIG of matters that pose an imminent or serious threat to NRC classified interests.

H. Physical Protection Facilities

1. Notification

   (a) Certain NRC facilities that are not designated “security facilities” must be designated “physical protection facilities” when they are within the scope of the specific security criteria set forth in Section III of this handbook.

   (b) The responsible NRC office or division shall promptly notify DFS of any facility, contractor or otherwise, that is subject to this protection. This notification must include the name and address of the facility, its function, the nature of the interest, and the name and title of the individual responsible for its protection.

   (c) The responsible NRC organization also will notify DFS of any termination or significant change in the interest at any facility previously reported.

2. Physical Protection Surveys

   NRC security representatives conduct the following onsite critical examinations of a physical protection facility to ensure safeguarding of property or sensitive NRC interests:

   (a) Initial Physical Protection Survey

   The first survey conducted after a facility has been designated as a “physical protection facility.”

   (b) Periodic Physical Protection Survey

   A survey conducted subsequent to the initial survey at a scheduled frequency or interval. The frequency is determined by the sensitivity, special circumstances, and local environment encompassing the facility. Continuity of Operations centers require, at a minimum, an annual physical security survey.

   (c) Special Physical Protection Survey

   A survey conducted to address specific problems, questions, or deficiencies and performed as necessary.

   (d) Termination Physical Protection Survey

   A survey conducted to confirm the termination of property or sensitive NRC interests.

I. Facility Data Reports and the Master Facility Register

DFS will maintain a Master Facility Register that lists the name and address of each facility with an NRC interest, the level of security approval, the responsible NRC contracting office or other office, the name and title of the security administrator, the current survey rating—“U” (unsatisfactory) or “S” (satisfactory)—and other pertinent information relative to the facility.

II. PHYSICAL SECURITY REQUIREMENTS FOR THE PROTECTION OF CLASSIFIED INFORMATION

A. Introduction

1. Section II provides the practices and procedures for the protection of classified information and facilities pursuant to the Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, as amended, and Executive Orders (e.g., Executive Orders 10865 and 12958, as amended).

2. Security measures for existing NRC facilities shall be in compliance with the guidance in the Department of Justice's (DOJ's) Vulnerability Assessment of Federal Facilities document. Security measures for new NRC facilities shall be in compliance with the Interagency Security Committee Security Criteria for New Federal Office Buildings and Major Modernization Projects or other applicable security standards, as determined by the Director of DFS, ADM.

3. In addition, specific security measures shall be implemented in response to the Department of Homeland Security announced threat conditions.

B. Overview of Physical Security

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. Physical security as it relates to the protection afforded classified information is composed of physical controls and administrative procedures used to adequately deter its unauthorized disclosure. DFS, ADM, establishes, maintains, and oversees these controls. Nothing in this directive and handbook shall be construed to contradict or inhibit compliance with laws and building codes applicable to life safety and the Americans With Disabilities Act of 1990.

1. Basic Considerations

   The factors to be taken into consideration in determining the type and degree of physical protection to be afforded classified information include—

   (a) The level of the classified information, such as Top Secret, Secret, or Confidential; the relative vulnerability of that information to espionage, sabotage, theft, or other unlawful activity; and the need for compartmentalization of the information.

   (b) The relative importance of the facility, or the information housed in the facility, to the overall NRC program, considering such items as the availability of alternate facilities and information that could be used in an emergency.

(c) The location, size, and arrangement of the facility that houses the classified information and the need to integrate security measures with facility operations.

(d) The relative efficiency, effectiveness, and economy of alternative methods of protection.

2. Access Controls and Authorization

(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.

(c) Persons without appropriate access authorization for the area visited must be escorted at all times by a person possessing the appropriate access authorization while within a security area or any other area in which unsecured classified information is located, such as open storage areas. Additionally, when there are local or unique restrictions on access because of operating, technical, or compartmentalization considerations, only persons knowledgeable of these restrictions shall serve as escorts. Persons without the appropriate access authorization do not require escort within nonsecurity areas or facilities when the classified information located in these areas or facilities is properly secured.

3. Control of Areas

Physical and administrative controls will be established and maintained to control access by individuals to certain predesignated areas to protect classified information located in these areas.

(a) Security Area

A security area is a physically defined space (usually a room, or a series of interconnecting rooms, within a facility) containing classified information and subject to physical protection and personnel access controls. A security area will be established when the nature, size, revealing characteristics, sensitivity, or importance of the classified information is such that access cannot otherwise be effectively controlled. Accordingly, entry into the security area must not be allowed if such entry will, in itself, constitute improper access to classified information.

(b) Controlled Area

(i) A controlled area is a space over which the NRC or an NRC contractor exercises administrative and physical control by use of properly cleared and authorized employees or guards stationed so as to control admittance to the

room, building, or structure, or by a lock that provides reasonable protection against surreptitious entry.

(ii) Entry into a controlled area must not, in itself, constitute access to classified information.

(iii) The Director of DFS, ADM, determines the nature and degree of the minimum controls necessary to establish and maintain controlled areas.

4. Package Inspection

Packages, parcels, briefcases, and any other similar containers will be subject to inspection before admittance to a facility. Inspections may include the use of metal detector equipment, X-ray equipment, explosives detectors, and/or hand-screening within standard security personnel guidelines. The purpose of this inspection is to ensure that prohibited articles are not admitted into the facility.

(a) Prohibited Articles

(i) Any article that could result in the illegal or covert compromise of classified or sensitive unclassified information or cause property damage or personal injury is prohibited. Prohibited articles include firearms, explosives, incendiary devices, or any other item similar in effect or purpose. Federal law, Title 41, *Code of Federal Regulations*, "Public Contracts and Property Management," prohibits the knowing possession or the causing to be present of firearms or other dangerous weapons in Federal facilities and Federal court facilities by all persons not specifically authorized by Title 18, *United States Code*, Section 930(d). Violators shall be subject to fine and/or imprisonment for a period up to five (5) years. Only upon request to and approval by the Director of DFS, ADM, his or her designee, or a regional administrator will an exception be permitted.

(ii) Use of NRC-owned recording, photographic, or other equipment in areas other than security areas issued expressly for the purpose of accomplishing official NRC business is not prohibited or restricted by this requirement. Individuals responsible for such NRC equipment shall take necessary actions to ensure that the equipment is not used in "security areas" or whenever it could knowingly or unknowingly compromise classified or sensitive unclassified information.

(iii) Portable electronic devices, including cameras, cellular telephones, pagers, palm-size computing devices, two-way radios, and portable computers, are allowed into NRC buildings and public meetings. However, the use of any device to take pictures inside NRC buildings is prohibited without prior approval by the Director of DFS, ADM. These devices shall be prohibited from sensitive compartmented information facilities (SCIFs) and classified meeting rooms. In addition, these devices shall be prohibited from other security areas

when classified meetings are being held. Devices that could interrupt or distract from public meetings (cameras, cellular phones, pagers, and two-way radios) are not to be used during public meetings.

(iv) Visitors may use recording devices in public meetings held in NRC headquarters spaces on the lobby levels designated as "public access areas." Cameras and video recording devices (e.g., camcorders) are permitted to be used in public meetings on a case-by-case basis, with the approval of the Director of the Office of Public Affairs, or the Director of DFS, ADM.

(v) Any article that could cause property damage or personal injury is prohibited in NRC buildings. Members of the public going to NRC "controlled spaces" inside the buildings above the lobby levels are allowed access with recording devices with the approval of the sponsoring office and under the escort of an NRC employee.

(vi) Persons who fail to adhere to NRC policy regarding prohibited articles will be denied access or detained for arrest by an appropriate law enforcement officer, as deemed appropriate by security personnel.

(vii) The prohibition on the admittance of a firearm, a two-way radio, or similar law enforcement equipment would not normally apply to Federal, State, or local law enforcement authorities whose duties require the possession of these articles.

(b) Notices

Written notices setting forth the policy and requirements regarding prohibited articles will be conspicuously posted at the entrance to the facility or area concerned.

(c) Special Considerations

Notwithstanding the above information, packages, briefcases, parcels, and any similar containers of any visitor, employee, or vehicle may be inspected whenever the Director of DFS, ADM, or a regional administrator decides that inspection is warranted.

(d) Possible Violations of Law

When inspection of a package, a box, a briefcase, or a similar container discloses a prohibited article and there is no reasonable explanation for its presence, the matter must be reported to the Director of DFS, ADM. Similarly, when there is an indication of a possible violation of Federal law, the matter must be reported immediately in accordance with Section V of this handbook.

5. Personnel and Vehicular Access Controls

(a) Positive Identification

Verification of the identity of persons authorized access to NRC security areas, or other areas as determined by the Director of DFS, ADM, will be accomplished at

the designated entry points by a guard, a receptionist, or other person assigned for that purpose. NRC and NRC contractor personnel shall present a valid NRC picture identification badge. The guard or receptionist shall require all visitors age 18 and older to present a valid picture identification, such as a driver's permit or passport, before issuing a temporary visitor's badge.

(b) Entrance Equipment

Entrances to NRC security areas, or other areas as determined by DFS, may be equipped with metal detector equipment, X-ray equipment and/or explosives detectors, doors, gates, rails, turnstiles or other movable barriers to screen, direct, and control personnel, packages, or vehicles through designated portals.

C. Personnel Identification System

A pass or badge system will be used to control access to security areas or any other area designated by DFS in which 30 or more people are employed. Such a system is used to ensure that only authorized persons enter or leave the facility or area concerned and to indicate any limitations placed upon access to classified information. DFS procures and issues the badges. NRC-badged individuals must conspicuously wear their badge at all times while in NRC-controlled space. Personal recognition may be used in lieu of a pass or badge system to control access to a facility in which fewer than 30 persons are employed.

1. NRC Permanent Identification Badge

(a) Badge Issuance

(i) To control access to NRC facilities, an NRC permanent picture identification badge is issued to all NRC employees, selected NRC contractors, and others, such as long-term visitors and other agency employees assigned to NRC.

(ii) The badge shall not be loaned to anyone. Misuse of a badge may result in a security infraction.

(b) Badge Confiscation

An NRC-issued badge may be confiscated by a guard or another NRC official when the Director of DFS, ADM, deems it necessary to deny the person access to the work site. Confiscation may become necessary when there is involvement or threat of involvement in a serious incident (altercation, misconduct, etc.) or other situation (i.e., life safety, national security threat) that in the best judgment of DFS necessitates the immediate removal and denial of the person from the work site until after an inquiry, investigation, or other appropriate action can determine that the person does not present a security or safety risk. Confiscation of a badge may also be necessary when a badged individual is denied access to the work site as a result of the individual's being placed on administrative leave,

being suspended or terminated, or if a personnel security clearance is suspended, denied, or revoked. Badge confiscation does not necessarily denote revocation of employment or security clearance.

(c) Badge Specifications

The face of the badge will contain the name and location of the issuing office, such as NRC Headquarters or the regional office; will be consecutively numbered to ensure accountability; and will be prominently coded by letter, number, or color to denote the level of access authorization, if any, held by the person. A clear image of the individual and his or her name will be displayed. The badge will be designed and made of materials to effectively prevent attempted alteration. Any additional specifications will be developed and approved by DFS.

(d) Badge Holder

The badge holder must meet the security requirement for an "electromagnetically opaque sleeve," derived from Section 2.4 of the Federal Information Processing Standards FIPS-201-1 standard and a subsequent National Institute of Standards and Technology special publication SP800-116, "Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)," to protect against any unauthorized contactless access to information stored on a PIV credential.

2. NRC Visitor Badges

(a) Temporary Visitor Badges

Temporary badges are issued to visitors and uncleared contractors who require one-time or short-term access to NRC facilities. This badge must be continuously and conspicuously worn by the visitor. Temporary badges must be inventoried and accounted for on a daily basis. The inventory of temporary badges will be stored in a locked cabinet when unattended to protect against loss, theft, or unauthorized use. An NRC temporary visitor badge will contain the following information:

(i) Level of access authorization, if any, prominently coded by letter, color, or number.

(ii) Escort requirement, if any.

(iii) A control number and/or date to ensure proper facility access and badge accountability/inventory control.

(b) Foreign Assignee Badges

Foreign nationals who are temporarily assigned to NRC will be issued a permanent identification badge that meets the specifications and requirements of Section I.C.1 of this handbook and contains the words "Foreign Assignee."

3. Temporary Badges for Employees

   Temporary badges for employees must conform to the requirements for permanent hard badges for employees or visitors. Temporary badges for employees must be returned to the guard or receptionist desk at the facility from which they were issued at the end of the work day.

4. Records

   Records must be maintained by each facility showing the disposition of all badges and passes in use or in storage. These records must include the date of issuance, the name of the holder, the type of access authorization and, if applicable, the categories of information and the areas within the facility to which access is permitted. Accountability for badges destroyed, scrapped, or returned must be maintained in accordance with agency records retention standards.

5. Lost Badges or Passes

   Each individual issued an NRC badge or pass is responsible for its protection. The loss or recovery of an NRC identification badge or pass must be reported immediately to DFS.

6. Return of Badges or Passes

   All NRC badges or passes issued must be returned to DFS upon the termination of an individual's employment or when the badge or pass is no longer needed for access to NRC facilities.

7. Reissuance of Badges or Passes

   To maintain effective security, all employee, contractor, and temporary badges or passes in use will be replaced by a badge or pass that is distinctly different in design approximately every 5 years.

8. Special Requirements for Security Areas

   The NRC badge or pass must be shown to the guard, receptionist, or other responsible individual before access can be gained to any NRC security area. Badges or passes must be conspicuously worn by all individuals while in any NRC security area. In some instances, or as required by DFS, separate entry registers or logs for the security area also will be used. All employees and duly authorized visitors will be informed of the special security requirements of each security area before being admitted to the area. This instruction is normally accomplished by the guard, the receptionist, or other responsible individual controlling access to the security area concerned.

9. Escort Passes and Instructions

   A guard or receptionist should issue oral or written instructions to escorts for visitors and uncleared contractors. The instructions should clearly outline the escort's responsibilities. As a general rule, one employee may escort up to five visitors and must keep the visitors within close proximity and sight at all times. In special cases (i.e., due to operational necessity), NRC badged contractors with building access can escort uncleared contractors, with the approval of the Director of DFS, ADM. Escorts should adhere to escort rules that have been approved by the Director of DFS, ADM.

D. Physical Barriers

1. Physical barriers such as walls, doors, fences, and electronic entry devices will be used to deny or impede unauthorized access to security areas or other areas as required by DFS. Permanent barriers will be used to enclose all security areas, and any other area as directed by DFS, except during construction when temporary barriers may be erected.

2. DFS will approve use of electronic and electro-mechanical devices to control personnel access (e.g., card reader entry controls) to supplement existing physical security requirements. These devices will be used at those facilities at which physical layout, level of classified information in use or in storage, and other factors demonstrate that these devices will effectively and efficiently control personnel access to the facilities. The following requirements will apply:

   (a) General Requirements

      (i) Entry control devices may be used, as approved above, to control access to NRC-owned or -leased space but must not be used as the sole personnel access control to security areas or other areas in which access to a room or a defined space would constitute access to classified information.

      (ii) NRC employees and others who have been authorized unescorted access and whose duties require daily or regular access to facilities or areas employing these devices will be issued the necessary control card or other medium needed to operate the devices.

   (b) Requirements for Visitors

      Visitors and uncleared contractors requiring access to an NRC controlled area must report to the appropriate guard or receptionist desk to complete the required visitor registration process. The guard or receptionist shall require all visitors age 18 and older to present valid picture identification, such as a driver's permit, a passport, or official Federal, State, or local government credentials. All visitors accessing controlled space shall be issued a visitor's badge that must be conspicuously worn at all times and visitors must be under continuous escort by an NRC employee or

other badged person approved by the Director of DFS, ADM, ADM. In special cases (i.e., due to operational necessity), NRC badged contractors with building access can escort uncleared contractors, with the approval of the Director of DFS, ADM. Upon completion of the visit, the visitor must be escorted to a public access area and the visitor's badge shall be turned in at the guard desk. Visitors who are authorized unescorted access will be issued a temporary control card or badge. Upon completion of the visit, the temporary control card or badge must be returned to the issuing guard or receptionist desk.

(c) Prohibitions

Permanent or temporary control cards/badges are not transferable and must not be used by any person who was not originally assigned the use of the card or badge. Failure to abide by this requirement will constitute a breach of established security regulations and may result in disciplinary action.

E. Intrusion Detection System

1. Interior Intrusion Detection Systems

As used in this section, devices and equipment for an interior intrusion detection system (IDS) required for the protection of classified information are tamper-indicating, electrical, electro-mechanical, electro-optical, electronic, or similar devices that will detect intrusion by an individual into the protected facility or area and will alert guards, watchmen, or other duly assigned personnel by means of actuated visible and audible signals. The Director of DFS, ADM, must approve the installation of an IDS. Approval of a new IDS shall be based on standards set forth in the Intelligence Community Standard No. 705-1, "Physical and Technical Security Standards (SCIFS)," or Underwriters Laboratory (UL) Standard 2050, as determined by the Director of DFS, ADM.

(a) Access Authorization Requirement

Facility protective personnel responding to intrusion detection alarms used for the protection of National Security Information or Restricted Data must possess "Q" or "L" access authorizations, except in those situations in which a commercial response force, located at a central alarm station outside the facility, is involved. In these instances, the responding commercial force must secure the perimeter of the area or facility until properly authorized facility protection personnel arrive. Section II.F of this handbook sets forth additional specifications for access authorization.

(b) Records

(i) When an IDS is used, it shall be activated immediately at the close of business at the alarmed area or container. This activation may require that the last person who departs the controlled area or checks the security container notify

the central alarm station to set the alarm. A record shall be maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate the IDS shall be reported to the central alarm station protective personnel. Such records shall be maintained for 30 days.

(ii) Protective personnel must document and maintain records for 90 days indicating a nonscheduled alarm, showing the date and time the signal was received, the time protective or other responsible personnel arrived at the alarmed area, the action taken, the cause of the alarm if known, or probable cause if the cause is not definitely established, and the followup actions that were accomplished. The name and signature of the recorder and the date of the recording must appear in the record.

(c) Reports

A report of each nonscheduled alarm containing the information required in Section II.E.1(b) of this handbook must be furnished to the facility security officer immediately if unauthorized intrusion is involved. Otherwise, the report will be furnished to the facility security office on the same day if the alarm occurs during normal working hours or no later than the first working day after the alarm if it occurs during nonworking hours. A violation or suspected violation must be reported to the Director of DFS, ADM, immediately in accordance with reporting procedures outlined in Section V of this handbook.

(d) Protection of Central Station Alarm System

(i) Facility central stations must be established as, or located within, security areas and must be constantly attended. Admittance must be restricted to those who require access in the performance of official duties. The number of personnel who require access must be kept to a minimum.

(ii) Commercial central stations must meet Grade “A” standards established by UL-611, “Central Station Burglar Alarm Units and Systems.” A copy of UL certification that a central station of a commercial protection service meets these standards will be accepted as evidence of compliance with the requirement.

(iii) Police central stations are normally attended continuously. If response by police to an alarm device is required for NRC facility approval, the central station should be one that is constantly attended by members of the police department who can direct a response by armed policemen to the alarmed area. In addition, the connection to the police central station should meet the specification contained in UL Class A of UL-365, “Police Station Connected Burglar Alarm Systems and Units.”

2. Protective Lighting

   (a) Protective lighting should be used, as appropriate, as part of a security system to properly protect a facility that houses classified information.

   (b) Adequate illumination must be provided at all times to detect intruders, reveal unauthorized personnel, and permit examination of credentials, personnel identification badges, and vehicles at pedestrian and vehicular entrances.

F. Protective Personnel

1. Guard Force

   A licensed and trained guard force is required for the protection of security areas in which classified information cannot be adequately safeguarded by employees during working hours or by alarm protection systems during nonworking hours as set forth in Section II.E of this handbook.

2. Guard force requirements (e.g., post orders, performance measures, and other qualifications) must be specified in contract documents.

G. Protection of Classified Information in Use

1. Requirements

   Persons using classified information in the performance of official duties shall physically protect the information to ensure that the information is safeguarded against unauthorized disclosure. The requirements specified below must be followed by all those who use classified information.

   (a) Visual Controls

   All classified information must be kept under the constant surveillance of an authorized person. As specified in Section II.H of this handbook, classified information must never be left unattended when in actual use or not secured in an approved storage area or container.

   (b) Personal Responsibility

   Those attending or controlling classified information in actual use shall prevent unauthorized persons from having access to the information. The information must be protected against visual access when the information can be obtained by observation. The information must be covered, turned face down, placed in approved storage containers, or otherwise protected when unauthorized persons are present. As applicable, drapes, blinds, shades, or other window coverings must be drawn to ensure that classified information in use is not viewed by unauthorized persons. Classified information must be returned to approved storage containers or areas as soon as practicable after use.

(c) Accountability

An accountability system must be maintained to promptly reveal when classified information is lost or unaccounted for. The approved NRC accountability system for classified information is specified in MD 12.2, "NRC Classified Information Security Program."

2. Destruction of Classified Information

(a) Classified waste shall be destroyed as soon as practical. This requirement applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material.

(b) When no longer needed, classified information may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizers (e.g., hammer mills, choppers, and hybridized disintegration equipment) to ensure that the content is changed so that the information is completely obliterated or destroyed. Classified material shall be destroyed by appropriately cleared persons who have a full understanding of their responsibilities. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. The method of destruction chosen must completely preclude recognition or reconstruction of the classified information involved and must be approved by the Director of DFS, ADM.

(c) Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. Shredding may be used if the shredding device has been approved by the Director of DFS, ADM. Approval of shredders for the destruction of paper may be based on the most current National Security Agency (NSA) performance requirements for High Security Crosscut Paper Shredders, which may include equipment on the NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders or other supplemental means as deemed appropriate by the Director of DFS, ADM. Electronic media/equipment and microfilm/microfiche containing classified information or Safeguards Information are to be destroyed as directed in MD 12.5, "NRC Automated Information Security Program," Part II, Section 2.6.12, "Destruction of Storage Media," or sent to DFS, ADM for destruction. Before destroying classified waste, persons should refer to MD 12.2, "NRC Classified Information Security Program," Part I, for itemized destruction procedures for Top Secret, Secret, and Confidential information.

3. Classified Conferences

(a) Basic Considerations

Conferences involving classified information must be held within NRC-approved security areas whenever practicable. Classified conferences held outside security areas must only be held under conditions in which adequate protection can be provided for the classified information and with authorization by the Director of DFS, ADM.

(b) Request for Authorization

(i) Requests to hold classified conferences outside NRC security areas should be submitted to the Director of DFS, ADM, at least 15 days before the date of the conference and must contain the following information, as appropriate:

- Purpose and nature of the conference,
- Number of participants,
- Specific location of the conference, building and room number,
- Level and category of the classified information involved,
- Description of existing security restrictions concerning the classified information involved,
- Name of person(s) responsible for the security of the conference,
- Description of the conference area, adjacent rooms or areas, and the security precautions planned, and
- Information concerning any permanently installed public address systems, telephones, or other known situations or fixtures of possible concern to the security of the conference.

(ii) **Special Note**: Requests to hold classified conferences outside security areas must be marked and handled as Official Use Only information, except in those instances in which the request contains classified information necessitating security classification and control.

(c) Other Considerations

The conduct of a classified conference will be based on the following principles:

(i) All attendees must be named on the list of attendees and have the appropriate access authorization and need-to-know. The requirements of MD 12.3, “NRC Personnel Security Program,” Part II, as applicable, also must be met.

(ii) Unless specifically authorized by DFS, all attendees at such events must be U.S. citizens.

(iii) The level of classified information discussed is not to exceed Secret National Security Information (S-NSI) or Secret Restricted Data (S-RD) level without taking place in a SCIF or designated Top Secret discussion area.

(iv) Before classified information is introduced into a conference situation and as needed throughout the conference, the individual responsible for the security of the conference shall advise those present of the restrictions governing the information. Additional instructions governing the security of the information, such as the permissibility of taking written notes, must be provided as necessary. The person conducting the meeting must also advise attendees that all recording and transmitting electronic equipment is prohibited in the room during the meeting unless specifically authorized.

(v) The room perimeter must be monitored to protect from unauthorized entry, and all windows must be covered.

4. Prevention of the Use of Surreptitious Listening Devices

(a) Offices or rooms within NRC security areas in which Top Secret information is discussed on a regular or recurring basis must be inspected periodically by DFS to ensure that classified information will not be compromised by surreptitious listening devices. The person assuming cognizance over the classified conference shall contact DFS at least 10 workdays in advance to arrange for security inspection of the office or room.

(b) Conference rooms located outside NRC security areas must be inspected by DFS immediately before any conference involving Top Secret information. Conference rooms used for discussions of Secret information must be inspected periodically and immediately before any Secret discussion.

(c) Appropriately cleared and qualified U.S. Government personnel or contractors must conduct all inspections of telephone equipment and public address systems.

(d) Telephones or public address systems in conference rooms or offices in which classified discussions regularly occur should be equipped with jacks or other disconnecting devices. Telephones and public address systems must be disconnected when classified discussions are taking place.

5. Reproduction of Classified Information

(a) Classified reproduction shall be accomplished by an authorized individual with knowledge of the procedures for classified reproduction. Reproduction of classified information must be accomplished under appropriate security conditions to preclude unauthorized access. For example, reproduction must not take place in the presence of uncleared persons, and care must be taken that no classified waste is trapped in the equipment.

(b) Machines repeatedly used for reproduction of classified information should be located within a security area and protected against unauthorized access during nonworking hours. Notices regarding the restrictions and requirements of reproducing classified information must be conspicuously posted next to the equipment, and these requirements shall be strictly observed. Obtain copies of these notices from DFS, ADM, or NSIR.

(c) Maintenance personnel not authorized for access to the information processed by the copier shall be escorted and closely observed by a qualified and cleared individual.

H. Storage of Classified Information

The classification level of classified information determines the protection required for storage.

1. Security Containers

Security containers for Top Secret and Secret information must, as a minimum, be one of the following types:

(a) Security Filing Cabinet

A security filing cabinet bears a Test Certification Label on the side of the locking drawer, inside the wall adjacent to the locking drawer, or on an interior door plate, or is marked “General Services Administration Approved Security Container” on the exterior of the top drawer or door.

(b) Safe

A safe is a container that meets Federal Specification AAF-358 and bears a label of the Underwriters Laboratories, Inc., certifying the unit to be a TL-15, a TL-30, or a TRTL-30, or bears a Test Certification Label on the inside of the door, or is marked “General Services Administration Approved Security Container,” exclusive of bolt work and locking devices.

(c) Vault

A vault is a windowless enclosure constructed with walls, floor, roof, and door(s) that will delay penetration sufficient to permit the arrival of emergency response forces capable of preventing theft, diversion, damage, or compromise of the classified information when delay time is assessed in conjunction with detection and communication subsystems of the physical protection system.

(d) Vault-Type Room

A vault-type room has a combination lock door and is protected by an intrusion alarm system that alarms upon the unauthorized penetration by a person anywhere into the room.

(e) Other Repositories

Other repositories are those that would provide comparable physical protection in the judgment of DFS.

2. Requirements for Storage

The General Services Administration (GSA) establishes and publishes uniform standards, specifications, and supply schedules for security containers, vaults, key-operated and combination padlocks, and associated security devices suitable for the storage and protection of classified information and material throughout Government.

(a) Classified National Security Information

The Information Security Oversight Office (ISOO) Classified National Security Information Directive No.1, pursuant to Section 5.1 (a) and (b) of Executive Order 12958, "Classified National Security Information," as amended, (or any succeeding Executive Order and amendments), specifies the requirements for the storage of classified national security information. These requirements are published in 32 CFR 2001.43 (Exhibit 3).

(b) Communications Security Information

While unattended or not in use, Communications Security (COMSEC) information must be stored in a manner authorized above for the classification involved and storage must meet the standards and specifications set forth in NACSI-4005 (published by the National Security Agency, Department of Defense) and MD 12.4, "NRC Telecommunications Systems Security Program."

(c) Sensitive Compartmented Information

SCIF facilities must be afforded physical protection as required by Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," dated December 1, 2005. Matters pertaining to security requirements for these facilities must be directed to the Director of DFS, ADM, for coordination.

(d) Repository Checks

When guards or watchmen are required for the protection of NRC classified information in facilities housing unalarmed repositories containing Secret or Confidential information, the guards or watchmen shall—

(i) Physically inspect these repositories as soon as possible after the close of each working day and at least once every 8 hours during a Saturday, Sunday, holiday, or other nonworking day.

(ii) In the case of repositories located within security areas, physically inspect the entry into the security area or the repository itself, whichever applies, at intervals not to exceed 6 hours.

3. Alternate Storage Locations

(a) Safe deposit boxes or vaults of a bank may be used for storage of Secret or Confidential information provided that the lock and keys to the box or vault are changed before use and the customer's key is furnished only to those authorized access to the contents. These persons shall be appropriately cleared for the level of classification involved.

(b) Remote storage facilities, such as an offsite emergency relocation center or an underground Federal facility in a remote location, must be equipped with security containers for the storage of classified information and must otherwise meet the requirements of Section II.I.2 of this handbook.

(c) DFS can arrange for the storage of NRC Secret and Confidential documents in certain Federal Records Centers (FRCs). Among other necessary conditions for this storage are approval by GSA for storage of the category and level of classified information involved and DFS approval of the FRC facility in accordance with Section I of this handbook. If a problem involving volume storage of classified documents can be alleviated by FRC storage, contact DFS for additional guidance.

4. Miscellaneous Storage Specifications and Procedures

(a) Combination Locks

(i) A combination lock is a three- or four-position, dial-type combination lock meeting Federal Specification FF-L-2740.

(ii) A combination padlock is a three-position, dial-type, changeable combination padlock meeting Federal Specification FF-P-110.

(iii) Combinations of locks or padlocks on repositories containing classified information may be known only by those authorized access to the information. Such combinations must be changed when repositories are placed in or out of use; whenever anyone knowing the combination terminates employment or has their clearance withdrawn, suspended, or revoked; whenever the combination may have been compromised; following the discovery of a container left unlocked and unattended; or at least every 3 years. Annotating security container combinations on notepads, calendars, slips of paper in wallets or purse, personal electronic devices, and so on, is prohibited. See Section II.I.4(c) of this handbook for additional information regarding combinations.

(iv) Records of combinations must be classified no lower than the highest classification of the information stored in the repository.

(b) Lock Bars, Keys, Hasps, and Yokes

(i) Lock bars must be 1-1/4 inches by 3/16 inch or equivalent in cross-section and constructed of hardened steel or a material of equivalent hardness.

(ii) Hasps and yokes on repositories containing classified information must be constructed of hardened steel at least 1/4 inch in diameter or equivalent cross-section and secured to the repositories by welding or riveting.

(iii) Keys to locks used to secure gates or doors in the perimeters of a security area must be issued only to those authorized access to the information or to the area. Keys must be given protection equal to that afforded the information or item being protected. A record of all locks, cores, and keys must be maintained. Keys must be recovered from terminating personnel. Locks must be changed or the key or lock compromise recorded immediately whenever a key is lost, the key or lock has been compromised, or when unrecorded keys are found. A physical inventory of locks, cores, and keys must be conducted annually.

(c) Locking and Monitoring of Repositories and Office Areas

(i) Each office must assign personnel to lock and monitor the locking of all repositories containing classified information and to ensure that all classified information is properly secured when the office is unattended.

(ii) The names, addresses, and home telephone numbers of custodians having knowledge of the combination and the date of the last combination change must be posted on the inside of each classified repository on Part I of SF 700, “Security Container Information” (Exhibit 4). Part 2A contains the combination of the repository and must be classified at the highest level of the information authorized for storage in the repository. Part 2 must be similarly classified at the highest level of the information authorized for storage in the repository when it contains the combination. A new SF 700 must be completed each time the combination of the repository is changed.

(iii) SF 702, “Security Container Check Sheet” (Exhibit 5), must be posted on each repository containing classified information. Whenever a security container is opened, the check sheet must be initialed at the end of the day in the “closed by” block by the person responsible for locking the repository and in the “checked by” block by one other person who has physically checked the repository to ensure that it has been properly secured. If no other person is available, the person locking the repository will recheck the repository and initial the “checked by” block as well as the “closed by” block.

(iv) Security containers that must be removed for repair or maintenance, that are to be returned to the supply system, or that are taken out of service for any reason

must be physically examined by the custodian of the container before this action to ensure that no classified information is mistakenly left in the container. Any built-in combination lock must be reset to the standard combination 50-25-50. Combination padlocks must be reset to the standard combination 10-20-30.

(v) Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers. An approved container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer's replacement or identical cannibalized parts. GSA-approved security containers that cannot be repaired in a GSA-approved manner will not be considered to have been restored to its original state of security integrity. In such cases, the test certification label on the inside of the locking drawer and the GSA-approved security container label, if any, on the outside of the top drawer will be removed from such containers, and the container shall no longer be used for the storage of classified information.

(d) Unattended Repository Found Open

(i) In the event an unattended repository containing classified information is found open, a card, "Notice of Unlocked Condition—Classified Matter Container," is placed in the repository, the repository is secured by a designated person such as a guard or watchman, and the custodian shall check the contents not later than the next workday.

(ii) If there is an indication of a suspected violation (see Section V of this handbook) by NRC employees or contractors, it must be reported immediately to DFS, ADM, and OIG. Personnel must secure the area, being careful not to destroy any criminal evidence, but independent investigations shall not be conducted before notifying DFS and OIG.

I. Trespassing on Commission Property

1. Statutory Provisions

Pursuant to the authority of Section 229 of the Atomic Energy Act of 1954, as amended, 10 CFR Part 160 prohibits the unauthorized entry and the unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any designated and posted facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Commission. The statute provides penalties for violations.

2. Criteria

   Selection of facilities, installations, and real property for posting will generally be based upon the need for supplementing other Federal statutes protecting against espionage, sabotage, or destruction of Government property. Real property may be posted for protection for reasons other than the protection of classified information if deemed necessary.

3. Proposals

   (a) Submission

   Proposals for the posting of facilities, installations, or real property, or amendment to or revocation of a previous proposal, will be submitted when—

   (i) The property is owned by, or leased to, the United States for use by the NRC.

   (ii) The property requires protection under 10 CFR Part 160.

   (iii) A previous notice needs to be amended or revoked.

   (b) Contents

   (i) Each proposal for posting will contain the name and specific location of the installation, facility, or real property to be covered, and the boundary coordinates. If boundary coordinates are not available, the proposal will include a description adequate enough to furnish reasonable notice of the area to be covered, which may be an entire area or any portion thereof that can be physically delineated by the posting specified in Section II.I.4 of this handbook.

   (ii) Each proposal for amendment or revocation will identify the property involved; state clearly the action to be taken, such as a change in property description, correction, or revocation; and contain a new or revised property description, if required.

4. Posting Requirements

   (a) Upon approval by the Executive Director for Operations (EDO), the notice designating the facility, installation, or real property, or amending or revoking a previous notice, will be published in the *Federal Register*. The regulation will be effective 30 days after publication, provided the posting requirements are met.

   (b) If directed by the EDO, property covered under 10 CFR Part 160 will be posted at entrances and at intervals along the perimeter of the property to provide reasonable assurance of notice to persons about to enter the property. Signs will measure at least 11 by 14 inches and follow the example provided in Exhibit 6.

5. Notification to the Federal Bureau of Investigation

   Notification of the date of posting, relocation, removal of posting, or other change in the identity of the property involved must be furnished promptly to the local office of the Federal Bureau of Investigation (FBI) exercising investigative responsibility for the property.

6. Violations

   Violations of the prohibitions as posted must be reported in accordance with Section V of this handbook.

III. PROTECTION OF UNCLASSIFIED NRC FACILITIES

A. Introduction

Section III provides guidance for those responsible for the protection of NRC facilities that are not protected as security facilities under Section I of this handbook but that require safeguarding to ensure adequate protection of NRC property and programs.

B. Criteria

1. Facilities that are not protected as security facilities under Section I of this handbook require protection commensurate with their monetary value or programmatic importance. For the purposes of this section, an unclassified NRC facility requiring protection is any facility that—

   (a) Contains property, excluding real property, owned by or leased to the NRC, valued at $1,000,000 or more.

   (b) Contributes in an important manner to fulfilling NRC's responsibility for the protection of public health or safety.

   (c) Assumes importance for continuity of NRC programs or is essential to the NRC mission.

   (d) Is determined by the Director of DFS, ADM, for headquarters facilities or by the responsible regional administrator for facilities within the region's geographical area of responsibility to require protection for other reasons.

2. When the relative importance of an unclassified NRC facility does not fall under these criteria, the facility must be protected to a degree called for by its value and significance. The extent of and need for protective measures at such a facility must be determined by the appropriate responsible NRC official, either the Director of DFS, ADM, for a headquarters facility or the regional administrator for a regional facility.

C. Guidance

1. General

Protective measures must be taken to prevent loss, damage, or destruction that might result from theft, vandalism, arson, sabotage, or other unlawful acts at unclassified NRC facilities. The measures taken must be adequate to provide reasonable assurance of protection and may include access controls; physical barriers, such as walls and fences; guards or watchmen; lock and key systems; and intrusion alarms.

2. Standards and Requirements

(a) Access Controls

Access to an unclassified NRC facility must be controlled during working hours by receptionists or by employees who have been specifically designated responsibility for ensuring that only those with proper authorization are admitted. When the facility is unoccupied, such as during nonworking hours, or occupied by a small number of persons unable to afford adequate protection, these facilities, as a minimum, must be locked with NRC-approved locking devices and must be protected by other means, such as NRC-approved access control devices, designated by the Director of DFS, ADM, or the responsible regional administrator, as appropriate.

(b) Physical Barriers

Barriers such as walls and fences are intended to control or impede access. Walls of buildings normally constitute an adequate physical barrier. When the size or nature of the facility warrants, fencing may be required and must be approved by the Director of DFS, ADM, or the regional administrator.

(c) Guards or Watchmen

Protection may be provided by guards or watchmen as the Director of DFS, ADM, or the responsible regional administrator deems necessary. When guards or watchmen are used, patrols must be conducted at irregular intervals but not less frequently than once every 8 hours during nonworking or unoccupied periods.

(d) Locks and Keys

Key locks in doors must be resistant to picking and jimmying. Combination locks must be resistant to manipulation. Padlocks must be of sturdy construction and resistant to picking, rapping, forcing, or the use of shims or similar techniques. Hasps and other door hardware must afford equivalent protection, as appropriate. Positive control of keys is essential. When an exterior or outer perimeter entrance key or door key is lost and there is reason to believe it has been compromised, the lock that it opens must be replaced or the loss or compromise must be recorded immediately. Combinations or keys and cores of exterior entrances or doors must be changed when a person having access thereto is terminated or the person is permanently reassigned to another

facility. Whenever 5 percent of the keys are lost or whenever the management official responsible for the area deems it appropriate, locks must be replaced, the loss or compromise (e.g., loss of the threshold number of keys) recorded, or combinations changed for interior doors. Advice on approved locks is available from DFS.

(e) Intrusion Alarms

Alarm systems may be used to provide or supplement notification of an actual unauthorized entry into an NRC facility or onto its premises. An intrusion alarm system is considered to be of significant value when a response time not exceeding 15 minutes is ensured and when the system itself is dependable. DFS can advise on alarm systems.

(f) Prohibited Articles

Inspection of packages to ensure that prohibited articles are not introduced into the facility must be accomplished as specified in Section II of this handbook.

(g) Post “No Trespassing” Signs

Facilities owned or leased by NRC must have signs posted as specified in Section II.I.4 of this handbook.

(h) Reports

Incidents bearing on the security of the facility, such as fire, vandalism, bomb threats, riots, or civil disturbances, must be reported immediately to DFS by telephone and also to the responsible regional office, if appropriate. This report must be promptly followed up in writing and must be initiated by the responsible NRC organization monitoring NRC's interest at the facility.

(i) Surveys

Physical protection surveys of unclassified NRC facilities must be conducted as specified in Section I of this handbook.

D. Occupant Emergency Program

In accordance with Federal Property Management Regulations promulgated by GSA (41 CFR 101-120.5, “Federal Property Management Regulations”), an occupant emergency program must be established at NRC-occupied facilities.

1. Occupant Emergency Plan

(a) An occupant emergency plan (OEP) specifies responses in an emergency situation and methods to protect life and property in a specific federally occupied space. For NRC headquarters-related buildings, OEPs are developed and coordinated by DFS and approved by the Director of ADM and local fire and rescue authorities. NRC regional offices shall develop, coordinate, and seek approval of their OEPs through

their local GSA regional office. (Reference Homeland Security Presidential Directive (HSPD) 3, "Homeland Security Advisory System").

(b) The OEP for each headquarters building is located on the NRC intranet Web page at http://www.internal.nrc.gov/ADM/documents/oep.pdf. Regional offices' OEPs are found at http://www.internal.nrc.gov/security.html.

2. Designated Official

As defined in 41 CFR 101-120.5, the designated official is the highest ranking official of the primary occupant agency or the alternate highest ranking official or designee selected by mutual agreement by other occupant agency officials. The designated official is responsible for developing, implementing, and maintaining a current OEP and for establishing, staffing, and maintaining the occupant emergency organization.

3. Occupant Emergency Coordinator

The Occupant Emergency Coordinator (OEC) is the on-scene person in charge of emergency response activities, including movement of occupants. He or she shall be easily identifiable by wearing an orange vest labeled "Occupant Emergency Coordinator."

E. Non-Federal Facility Emergency Plan

To ensure that emergency situations are appropriately provided for, non-Federal facilities, such as those of an NRC contractor, falling within the purview of this section must establish an adequate emergency plan to provide for the prompt assistance of Federal, State, and local law enforcement authorities and other emergency assistance organizations. DFS will review and approve this emergency plan during physical protection surveys and will advise as to the specific content of the plan on a case-by-case basis. Generally, these plans cover—

1. The emergency chain of command.
2. Designation of specific individuals, with alternates, who are responsible for key emergency functions and for notifying DFS or the appropriate regional administrator of incidents bearing on the security of the NRC interest at the facility.

IV. SECURITY AWARENESS

Section IV specifies the policy and requirements for a Security Awareness Program to develop an appreciation for the importance of security and the importance of potential threats to security; provide employees with an understanding of security policies, procedures, and requirements; advise employees of their security responsibilities; and ensure adequate protection for classified and sensitive unclassified information and NRC property.

A. Program Design

1. The program must be developed and implemented with careful consideration of—

   (a) The categories and quantities of classified or sensitive unclassified information handled and the personnel involved.

   (b) The physical security aspects of the facility.

   (c) Existing personnel security access authorization requirements.

2. The program must employ methods that are appropriate and effective for the personnel and situations concerned. The methods may range from informal instruction of individuals to audiovisual presentations for large groups. Briefing presentations by individuals skilled in public speaking and the use of constructive instruction techniques, such as visual aids and audience participation, are essential as they increase employee interest, motivation, and knowledge retention.

3. The program must contain—

   (a) An initial security orientation briefing for new and newly assigned employees.

   (b) A briefing on safeguarding classified and sensitive unclassified information for newly cleared employees.

   (c) Continuing and special security awareness efforts.

   (d) A final briefing upon termination of an individual's NRC access authorization.

B. Program Components

1. Security Orientation Briefing for New Employees

   A security orientation briefing must be given by an employee or a representative of DFS to NRC employees when they start duty and by the contractor security officer to contractor employees who have been granted an NRC access authorization (reference Executive Order 10865). This briefing will contain the following information—

   (a) The types of security clearances granted by the NRC and the access those clearances afford after an official need-to-know has been established.

   (b) Personnel security reporting responsibilities of each individual.

   (c) Overview of the security classification system, including prescribed procedures for the storage and handling of sensitive unclassified information and the importance of protecting this information.

(d) Physical security aspects of the particular facility, the importance of visitor control, and the means or procedures for protecting Government property.

(e) Information on where to obtain further guidance or assistance.

2. Briefing on Safeguarding Classified Information

A briefing on safeguarding classified information will be given by an employee or a representative of DFS or NSIR to NRC employees who have been granted an NRC access authorization. This briefing will contain the following:

(a) Requirements for access to classified information.

(b) Types and levels of classified information.

(c) Prescribed procedures for the storage, handling, and transmission of classified information and the importance of protecting this information.

(d) Information on where to obtain further guidance or assistance, such as MD 12.1 or consulting an authorized classifier or a security advisor.

(e) The requirement for signing an SF 312, “Classified Information Nondisclosure Agreement.”

(f) How to report a possible Infraction.

3. Continuing Refresher or Special Security Awareness Efforts

DFS or NSIR shall periodically reinforce the information provided during the initial security briefing, including changes in security regulations. This periodic training for all employees may be satisfied by the use of formal briefings, audiovisual materials, or written documents. This program should be reviewed and updated every 3 years.

(a) Security Advisor Program

The objectives of the Security Advisor Program are to increase the understanding of and compliance with NRC security policies and procedures; to provide readily available security advice and assistance throughout the NRC organization; and to expand communications between DFS and NRC employees. One or more employees from each NRC organizational component and the regional offices are appointed to serve as security advisors for the employees of their organizational component or region. DFS will adequately acquaint these individuals with basic and general NRC security policies and procedures and the staff and functions of DFS. Further, DFS will keep the security advisors informed of revision to security procedures and requirements and items and occurrences of security interest or concern.

(b) On-the-Job Security Training

Supervisors shall supplement the Security Education and Awareness Program through demonstrated endorsement of security principles and procedures, and by providing specific on-the-job instructions pertinent to the sensitivity of the employee's position and duties, such as protection requirements for information handled. Also, any physical security procedures particular to the office will be explained.

(c) Special Briefings

DFS or NSIR shall develop and present special briefings (e.g., Threat Awareness Briefings, Defensive Security Briefings) as requested by management, when a specific need is recognized, or in support of other security programs such as the Authorized Classifiers Program. Contractor security officers should contact DFS when special briefings are requested or considered.

(d) Defensive Security Briefings

Through various security education efforts, NRC and contractor employees who have been granted an NRC access authorization will be encouraged to contact the NSIR Information Security Branch when they contemplate travel, either official or personal, to designated countries or attendance at any international meeting, conference, or symposium so they can be given a defensive security briefing.

(e) Publications and Other Media

Publications and other media, such as posters, audiovisual productions, and booklets, may be used in support of the Security Awareness Program to increase employee awareness, employee motivation, and program effectiveness.

4. Briefing on Termination of Access

When an individual's NRC access authorization is to be terminated in accordance with MD 12.3, DFS, or designated regional staff, will conduct a termination briefing to inform the individual of his or her continuing security responsibilities. After all statements contained in NRC Form 136, “Security Termination Statement,” have been reviewed, the terminating individual and the person conducting the briefing shall execute the form.

C. Program Records

1. NRC employees and contractors to whom an access authorization has been granted shall complete an SF 312, “Classified Information Nondisclosure Agreement,” upon attendance at the briefing on safeguarding classified information and an NRC Form 136 upon termination of NRC employment. The original copy of these completed forms will be forwarded to DFS for retention.

2. NRC contractors shall maintain records of an employee's orientation, refresher, or special security briefings related to NRC work performed, and of the termination briefing, for 1 year after termination of the employee's NRC access authorization. The original copy of the completed NRC Form 136 must be forwarded to DFS for retention in the employee's personnel security file; the original copy of the completed SF 312, if applicable, must be forwarded to DFS for retention.

V. INFRACTIONS AND VIOLATIONS

A. Introduction

Section V contains the requirements, standards, and procedures governing the NRC Security Infraction Program, alleged and suspected violations of laws of security interest, and losses and compromises of classified and sensitive unclassified information.

B. Infractions

1. Security Infraction

   A security infraction is an act or an omission involving failure to comply with NRC security requirements or procedures. Therefore, an infraction may include an actual or a suspected compromise of classified information or sensitive unclassified information. A security infraction also may constitute a violation under this section. Some examples of an infraction are—

   (a) Leaving classified documents or material exposed and unattended or unsecured.

   (b) Improper storage of classified information or material.

   (c) Improper transmission of classified documents or material.

   (d) Permitting an unauthorized person to hear, obtain visual access to, or otherwise obtain classified information.

   (e) Unattended and unsecured classified security container.

   (f) Failure to properly safeguard a classified combination.

   (g) Failure to properly escort uncleared visitors.

   (h) Loss of pass or badge under circumstances of negligence.

2. Administrative Action

   Administrative action, which may include disciplinary or adverse action, may be taken in any case in which a person is responsible for an infraction.

(a) Determination of Action

(i) NRC Employees

Office or division directors at headquarters or regional administrators shall determine whether an infraction committed by an NRC employee requires disciplinary or adverse action and, if so, the severity of the action. The responsible director or administrator shall consult with the personnel office about any contemplated adverse action.

(ii) NRC Contractor Employees

The contractor's representative should consult with the NRC Project Officer to obtain any relevant information concerning a security infraction committed by a contractor employee. However, the contractor's representative shall be solely responsible for determining whether an infraction committed by an NRC contractor employee requires disciplinary or adverse action and, if so, the severity of the action.

(iii) Personnel of Other Government Agencies

The NRC or the NRC contractor shall take the minimum action in the case of personnel of other Government agencies assigned to the NRC or to NRC's contractors for the first infraction as described in Section V.B.2(c) of this handbook, unless the first infraction significantly endangers national security or the security of the NRC program. For a first infraction that endangers security and for any subsequent infraction, the responsible NRC official or NRC contractor official shall report the infraction to the Government agency to which the employee is permanently assigned to allow that agency to take the disciplinary or adverse action deemed necessary.

(b) Determining Factors

For NRC personnel or NRC contractor employees, the following factors should be considered in determining the action to be taken on security infractions—

(i) The degree to which national security or the security of the NRC program is endangered.

(ii) The employee's performance, conduct, attitude, and past record of compliance with security regulations.

(c) Suggested Schedule of Administrative Action

Except in cases in which consideration is being given to suspending or terminating access authorization, the following schedule of administrative action is suggested for infractions occurring within any 12-month period.

(i) First Infraction

Interview the person committing the infraction to impress on that person the seriousness of the matter, determine the reason for the infraction, and call attention to pertinent regulations and office procedures. If necessary, modify office procedures to prevent a recurrence. A notation of the interview and a copy of the infraction report should be placed in the personnel security file of the person deemed responsible for committing the infraction. The following responsible officials will conduct the interviews:

- Regions
  - In the case of an NRC regional office employee other than the administrator, the interview will be conducted by the administrator or the administrator's designee.
  - In the case of an infraction committed by the administrator, the interview will be conducted by the person to whom the administrator is administratively responsible.
- Headquarters
  - In the case of a headquarters employee other than an office or division director, the interview will be conducted by the director, the deputy director, or the assistant director of the employee's office or division, unless these persons are involved in the infraction.
  - In the case of the deputy director or the assistant director, the interview will be conducted by the director.
  - In the case of an office or division director, the interview will be conducted by a person to whom the director is administratively responsible.
- Contractors and Other Organizations
  - In the case of a contractor employee or an employee of an organization other than NRC, the interview will be conducted by an official designated by the contractor or the organization involved.

(ii) Second Infraction

Interview the person committing the infraction as specified in Section V.B.2(c)(i) of this handbook and write a reprimand to the employee warning that another infraction may result in an adverse action, specifically, the employee may be suspended without pay. Place a notation of the interview and a copy of the written reprimand in the employee's personnel and security files.

(iii) Third Infraction

Interview the person committing the infraction as specified in Section V.B.2(c)(i) of this handbook, suspend the employee without pay for 3 working days, and provide the employee written notification that a subsequent infraction may result in removal from his or her position with the NRC and from Federal service. Place a notation of the interview, a copy of the written reprimand, and a copy of the suspension letter in the employee's personnel and security files.

(iv) Subsequent Infractions

Determine whether to propose the employee's removal for cause. If the employee's removal is not proposed, propose other appropriate adverse action, such as an additional suspension without pay. Document the action taken in the employee's personnel and security files.

3. Reporting Infractions

(a) NRC Employees

Office or division directors and regional administrators shall report, in writing, to DFS, ADM, each infraction involving NRC personnel, consultants, and others under their jurisdiction immediately following the infraction.

(b) Contractor Employees

A contractor shall report each infraction immediately following its occurrence, in writing, to DFS, with a copy to the NRC project officer. In addition, the contractor shall immediately notify the contracting officer that an infraction has occurred, the details of the infraction, and the name of person who committed it.

(c) Content of Reports

NRC or NRC contractors shall provide any associated written reprimand or notice with each report that has been issued and shall forward the report and attachments to DFS to be placed in the individual's personnel security files. The report must state—

(i) The full name of the individual involved;

(ii) The title of that individual's position and the name and title of his or her employer;

(iii) The type and level of information involved, if applicable;

(iv) The date, reason or cause, and nature of the infraction;

(v) Whether it is the first, second, third, or subsequent infraction within a 12-month period, if known; and

(vi) The corrective action taken.

4. Preliminary Inquiry

   Upon receipt of the report of an infraction, DFS, or personnel designated by DFS, such as regional personnel, may conduct a preliminary inquiry to determine the facts and circumstances surrounding the infraction, the person responsible, and the adequacy of security procedures within the organization in which the infraction occurred. If at any time during the course of the preliminary inquiry information is developed that suggests a violation may have occurred, the matter will be referred immediately to the OIG or the Office of Investigations (OI), as appropriate, for action. See Section V.C.3 of this handbook.

C. Violations

1. Violation

   (a) "Violation," as used in this section, covers criminal breach of the Atomic Energy Act of 1954; the Internal Security Act of 1950, when related to NRC activities; and Title 18 of the *U.S. Code* relating to—

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

   (ii) Sabotage, Sections 2151-57;

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

   (iv) Malicious mischief, Sections 1361-64;

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

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

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

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

   (b) Other Federal statutes related to national security, the security of the NRC program or facilities, or classified information.

2. Handling a Violation

   Alleged or suspected violations of the Atomic Energy Act and other Federal statutes affecting national security and the security of NRC or NRC contractors must be handled with a view to timely and effective action.

3. Reporting Procedures

   (a) Reports to DFS

   Except as stated in Section V.C.3(c) of this handbook, NRC or NRC contractor personnel shall immediately report alleged or suspected violations affecting

classified information, sensitive unclassified information, and the safety of NRC personnel or property to DFS for preliminary inquiry and further referral, if warranted.

(b) Reports to OIG and OI

OIG and OI will advise DFS of alleged or suspected violations of security interest reported directly to them.

(c) Reports to the Regional Administrators

For cases requiring prompt field response, NRC employees or NRC contractor personnel under the jurisdiction of a regional administrator shall report alleged or suspected violations such as sabotage, terrorism, or the theft of special nuclear material to the regional administrator. The regional administrator shall notify the local office of the FBI immediately for action and promptly advise OIG and, if appropriate, OI, and they will determine their own course of action, if any.

(d) Method of Reporting

To ensure timely reporting, the initial report will generally be oral; however, reports must immediately be confirmed in writing.

4. Content of Report

Reports that contain classified or sensitive unclassified information must be properly protected and marked with the appropriate classification and control markings. Reports of alleged or suspected violations not involving losses or compromise of classified or sensitive unclassified information discussed in Section V.D of this handbook must contain the following:

(a) A statement regarding the items and information involved;

(b) Names of personnel involved;

(c) Circumstances; and

(d) Action contemplated or taken.

5. Investigation of Violations

OIG is responsible, except as stated in Section V.C.3(c) of this handbook, for investigating and referring to DOJ, if necessary, alleged or suspected violations by employees of NRC or NRC contractors. OI is responsible, except as stated in Section V.C.3(c) of this handbook, for investigating and referring to DOJ, if necessary, alleged or suspected violations that licensees, applicants, and their contractors and vendors commit.

6. Assistance to Federal Law Enforcement Agencies

   The NRC will give Federal law enforcement agencies all appropriate assistance, including technical advisory assistance, as needed. Agents of the FBI must be granted admission to all areas and afforded access to any Restricted Data or other classified information or sensitive unclassified information necessary to the performance of their duties. They must be advised at the time of access, either oral or visual access, of the level and category of classification, or of the category of sensitive unclassified information, and the procedures required to protect the information. The availability of NRC badges and advance notification arrangements must be determined by agreements between the NRC and FBI offices involved.

7. Followup of Alleged or Suspected Violations of Security

   NRC followup will include coordination with FBI or other Federal law enforcement authorities. Followup will be accomplished so as not to interfere with any investigation the FBI or other Federal law enforcement agencies are conducting and will be coordinated between OIG or OI and DFS as their interests demand.

D. Reports of Loss, Compromise, or Suspected Compromise of Classified Information

1. Reporting Procedures

   Any NRC employee or NRC contractor employee who knows of the loss, compromise, or suspected compromise of classified information shall report that fact to DFS or the Information Security Branch, Division of Security Operations, NSIR, by the most rapid and secure means available. NSIR will be notified in cases involving COMSEC, Sensitive Compartmented Information (SCI), and other classified information for which NSIR is the primary user. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an inquiry or an investigation determines otherwise. Reports of loss, compromise, or suspected compromise of sensitive unclassified information shall be handled in accordance with guidance in MD 12.6, “NRC Sensitive Unclassified Information Security Program.”

2. Content of Report

   The report of a lost or compromised classified or sensitive unclassified document must contain the following information:

   (a) Title, type, and physical form of the document;

   (b) A brief description of the contents of the document;

   (c) Originator's name;

   (d) Any identification number and the date of the document;

(e) Level and category of classified information contained in the document;

(f) Names of the person to whom the document was charged and the person responsible for protecting the document;

(g) Last known location of document if a lost document is involved; and

(h) Known circumstances surrounding the loss or compromise of the document.

3. Action

Upon notification, DFS or NSIR, as appropriate, will conduct a preliminary inquiry, including a preliminary assessment of the damage to NRC's mission or national security. DFS or NSIR will refer the preliminary assessment to the EDO, OI, OIG, the Office of the General Counsel, or the Chairman, as warranted, and take any other appropriate action. Whenever the lost or compromised classified information has been originated by or is of interest to another Government agency, DFS or NSIR will notify each agency involved of the facts, circumstances, actions being taken by NRC, and pertinent findings.

4. Damage Assessment

(a) When Conducted

If, in the judgment of the Chairman, the EDO, NSIR, or DFS, after having reviewed the preliminary assessment regarding the compromise of classified information originated by or for NRC, damage to national security could reasonably be expected, DFS or NSIR will prepare a damage assessment and take any other action warranted by the damage.

(b) Content of Damage Assessment

(i) Damage assessments must be in writing and, as a minimum, contain the following information:

- Identification of the source, date, and circumstances of the compromise;
- Classification of the specific information lost;
- A description of the specific information lost;
- An analysis and statement of the known or probable damage to national security that has resulted or may result from the compromise;
- An assessment of the possible advantage to foreign powers resulting from the compromise;
- An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise; and
- An assessment of other appropriate corrective, administrative, legal, disciplinary, or adverse actions.

(ii) Damage assessments must also determine the following:

- Whether the classification of the information involved should be continued without change.
- Whether the specific information, or parts thereof, must be modified to minimize or nullify the effects of the reported compromise and the classification retained.
- Whether downgrading, declassification, or upgrading is warranted. (If these actions are warranted, promptly notify holders of the information of any change and obtain confirmation of receipt of notification.)

(c) Damage Assessment Involving Information From Other Government Agencies

Whenever a damage assessment incorporating information from NRC and one or more other Government agency is needed, DFS (for collateral classified information) or NSIR (for COMSEC, SCI, etc.) and personnel of the other agency shall agree upon the assignment of responsibility for their agency's portion of the damage assessment. If NRC and any other agency conduct separate damage assessments for the same infraction, the NRC and any other agency involved will exchange any information from their separate assessments that would affect another agency's information or interests.

(d) Compromise by Foreign Nationals

(i) Whenever DFS or NSIR deems it necessary to perform a damage assessment involving the compromise of U.S. classified information as the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, DFS or NSIR will immediately notify the FBI before the assessment of documents and obtain the concurrence of the FBI. DFS or NSIR will then request that the Office of International Programs (OIP) obtain the required information pertinent to the assessment through appropriate intergovernmental liaison channels.

(ii) If NRC and one or more other Government agencies are responsible for the assessment, OIP will arrange for joint preparation of the assessment with any other involved agency through appropriate channels before transmitting the request for joint preparation to the other agency.

5. Records Maintained

DFS, NSIR, OIG, and OI will, as appropriate, maintain appropriate records of each instance 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.

6. Actions Against Individuals

   (a) Administrative and Criminal Sanctions

   Persons determined to have knowingly made an unauthorized disclosure of classified information or who have refused to cooperate in the inquiry or investigation will be denied further access to classified information and may be subject to other administrative sanctions. If alleged or suspected violations of Federal statutes are proven, the administrative or criminal penalties of the statute apply.

   (b) Action When No Criminal Prosecution Is Contemplated

   Whenever an action, other than criminal prosecution, is contemplated against any person responsible for the compromise of classified information, DFS or NSIR (regarding investigations of licensees) will furnish its damage assessment to either OIG or OI.

   (c) Action Involving Criminal Prosecution

   When a damage assessment reveals that a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment will coordinate the contemplated prosecution with the DOJ, OIG, or OI, depending upon which office has jurisdiction, will coordinate any contemplated prosecution that involves NRC with the DOJ.

VI. PROHIBITIONS ON WIRETAPPING AND EAVESDROPPING DEVICES

A. Introduction

Section VI relates to surreptitious use of wiretapping or eavesdropping devices in conversations or wire (including wireless) transmission without the consent of any of the participants[1]

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

[1] For NRC policies and procedures related to consensual monitoring or recording of verbal or wire communications, see MD 2.3, “Telecommunications.”

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 of up to $250,000 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.

C. Services Available From the Division of Facilities and Security

1. Technical Inspection

   DFS, ADM, will, on request, provide for Technical Surveillance Countermeasures (TSCM) surveys and inspections, or other technical inspections of facilities or premises in connection with proposed meetings or otherwise to determine the presence of wiretapping or eavesdropping devices.

2. Notification

   If any such device or suspected wiretapping or eavesdropping device is discovered as a result of this inspection or otherwise, DFS must be notified immediately by the most secure and rapid means available. No tests or attempts at removal must be made by anyone who discovers the device or by other personnel advised of the existence of the device, except as authorized either by DFS, which will act in coordination with the FBI or OIG. The FBI will have primary authority relating to any devices.

3. Staff Assistance

   DFS will provide staff assistance in determining whether the object is in fact a wiretapping or eavesdropping device and/or in handling the device. Only DFS will procure or possess devices required for such technical inspections or conduct or authorize such inspections.

D. Actions to be Taken Upon Discovery of Devices

1. By Individuals

   The individual who discovers an actual or suspected eavesdropping or wiretapping device shall take the following actions:

   (a) Maintain silence or normal conversation in the area in which the device is operative in order to conceal the discovery of the device.

(b) Avoid touching or otherwise tampering with the device.

(c) Provide immediate and constant surveillance of the device at all times until relieved by DFS representatives or directed otherwise by the FBI or DFS. (This course of action will prevent any touching or tampering with the device or its unauthorized removal.)

(d) If the discoverer is alone, enlist assistance from the nearest responsible NRC employee, or the nearest responsible NRC contractor employee if a contractor location is involved, to ensure that the device is kept under surveillance while DFS is being contacted.

(e) As soon as measures have been taken to ensure constant surveillance of the device, notify DFS by the most secure and rapid means available outside the listening area for the device. (Notification by telephone is acceptable, provided the device is not located in a telephone closet or in any way connected to telephone wires. If a telephone cannot be used, the nearest security guard should be notified.)

2. By DFS

DFS will notify OIG if any alleged or suspected criminal violations are involved, and OIG will notify appropriate law enforcement authorities.

3. Classification

Since there are potential national security implications associated with the discovery or use of these devices, all pertinent information must be classified Confidential National Security Information until it is reviewed. If NRC authorized classifiers have determined that classified information is not involved, the information must be handled as “Official Use Only.” Documents containing classified or Official Use Only information must be marked accordingly.

E. Advance Approval of Attachment of Any Devices to Telephone or Other Telecommunications Equipment and Notice of Use

1. Consensual Monitoring

(a) Generally, the NRC allows the monitoring or recording of wire or oral communications only with the specific knowledge and consent of all parties to the conversation. Normally, this is accomplished through the use of NRC-issued speaker telephones.

(b) If a need arises for the use of any other devices with the capability of monitoring or recording conversations to be attached to an NRC telephone system, office and division directors shall obtain advance written approval from the EDO before initiating action for physical wiring attachments or inductive coupling to any

telephone or other telecommunications equipment that has the inherent capability of monitoring or recording voice messages, even when the device is normally used in routine maintenance or operation.

2. Non-Consensual Monitoring

   Except for properly authorized law enforcement activities by Federal criminal investigators, monitoring or recording of wire or oral communications without the knowledge and consent of all parties is prohibited.

3. Line Compatibility

   Any recording equipment attached to telephone or other telecommunications lines must meet line compatibility requirements of the company supplying the lines.

F. Instructions to NRC Employees and Contractor Personnel

NRC office and division directors shall ensure that NRC and contractor personnel under their jurisdiction are aware of and observe the procedures specified in this handbook. Similarly, the heads of NRC contractor organizations have the same responsibility regarding their personnel.

EXHIBITS

Exhibit 1 Certificate of Possession

This is to certify to the best knowledge and belief of _____

_____

(name of contractor, subcontractor, or other party)

that, with the exception of the items listed below, it has returned to authorized representatives of the Nuclear Regulatory Commission (NRC), or disposed of in accordance with NRC security requirements, all classified documents and classified material originated, produced, or received by the company in connection with work performed by it for NRC under _____except _____

(identify contract, subcontract, or other agreement)

_____

(identify documents and material retained, length of retention, and indicate classification of each item)

It is understood and agreed that—

(1) The listed items will retain their present classification until downgraded or declassified by NRC and will be safeguarded in accordance with NRC security requirements;

(2) Unauthorized disclosure of classified information is subject to criminal penalties, as provided for, for example, in the Atomic Energy Act of 1954, as amended, and/or the Espionage Act; and

(3) Any unaccounted-for classified documents or classified material or listed items exposed to unauthorized persons will immediately be reported to NRC or the Federal Bureau of Investigation in accordance with NRC security requirements.

Signature

_____

(For the (name of contractor, subcontractor, or other party to the agreement).)

Title_____

Date_____

Exhibit 2 Certificate of Nonpossession

This is to certify to the best knowledge and belief of _____
_____
(name of contractor, subcontractor, or other party)

that it has returned to authorized representatives of the Nuclear Regulatory Commission (NRC), or disposed of in accordance with NRC security requirements, all classified documents and classified material originated, produced, or received in connection with work performed for NRC under

_____
_____
(identify contract, subcontract, or other agreement)

Signature _____
(For the (name of contractor, subcontractor, or other party to the agreement).)

Title_____

Date_____

Exhibit 3 Requirements for the Storage of Classified National Security Information (32 CFR 2001.43)

Security Authority for NATO Instructions I–69 and I–70. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at §2001.53 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) An agency head who originates or handles classified information shall refer any matter pertaining to the implementation of this Directive that he or she cannot resolve to the Director, ISOO for resolution.

§2001.41 Responsibilities of holders [4.1].

Authorized persons who have access to classified information are responsible for:

(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;

(b) Meeting safeguarding requirements prescribed by the agency head; and

(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

§2001.42 Standards for security equipment [4.1].

The Administrator of General Services shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications and supply schedules for security equipment designed to provide secure storage for and destruction of classified information. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

§2001.43 Storage [4.1].

(a) *General.* Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) *Requirements for physical protection.* (1) Top Secret. Top Secret information shall be stored by one of the following methods:

(i) In a GSA-approved security container with one of the following supplemental controls:

(A) Continuous protection by cleared guard or duty personnel;

(B) Inspection of the security container every two hours by cleared guard or duty personnel;

(C) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation [Acceptability of Intrusion Detection Equipment (IDE): All IDE must be UL-listed (or equivalent as defined by the agency head) and approved by the agency head. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head.]; or

(D) Security-In-Depth conditions, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L–2740.

(ii) An open storage area constructed in accordance with §2001.43, which is equipped with an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth or a five minute alarm response if it is not.

Exhibit 3 Requirements for the Storage of Classified National Security Information (32 CFR 2001.43) (continued)

(iii) An IDS-equipped vault with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) Secret. Secret information shall be stored by one of the following methods:

(i) In the same manner as prescribed for Top Secret information;

(ii) In a GSA-approved security container or vault without supplemental controls; or

(iii) In either of the following:

(A) Until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock; or

(B) An open storage area. In either case, one of the following supplemental controls is required:

(*1*) The location that houses the container or open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(*2*) Cleared guard or duty personnel shall inspect the security container or open storage area once every four hours; or

(*3*) An IDS (per paragraph (b)(1)(i)(C) of this section) with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation. [In addition to one of these supplemental controls specified in paragraphs (b)(2)(iii)(B)(*1*) through (*3*), security-in-depth as determined by the agency head is required as part of the supplemental controls for a non-GSA-approved container or open storage area storing Secret information.]

(3) Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

(c) *Combinations.* Use and maintenance of dial-type locks and other changeable combination locks.

(1) Equipment in service. The classification of the combination shall be the same as the highest level of classified information that is protected by the lock. Combinations to dial-type locks shall be changed only by persons having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

(i) Whenever such equipment is placed into use;

(ii) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or

(iii) Whenever a combination has been subject to possible unauthorized disclosure.

(2) Equipment out of service. When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the built-in combination lock shall be reset to a standard combination.

(d) *Key operated locks.* When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established.

§ 2001.44 Information controls [4.1, 4.2].

(a) *General.* Agency heads shall establish a system of control measures which assure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(b) *Reproduction.* Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken:

Exhibit 4 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

Front Side

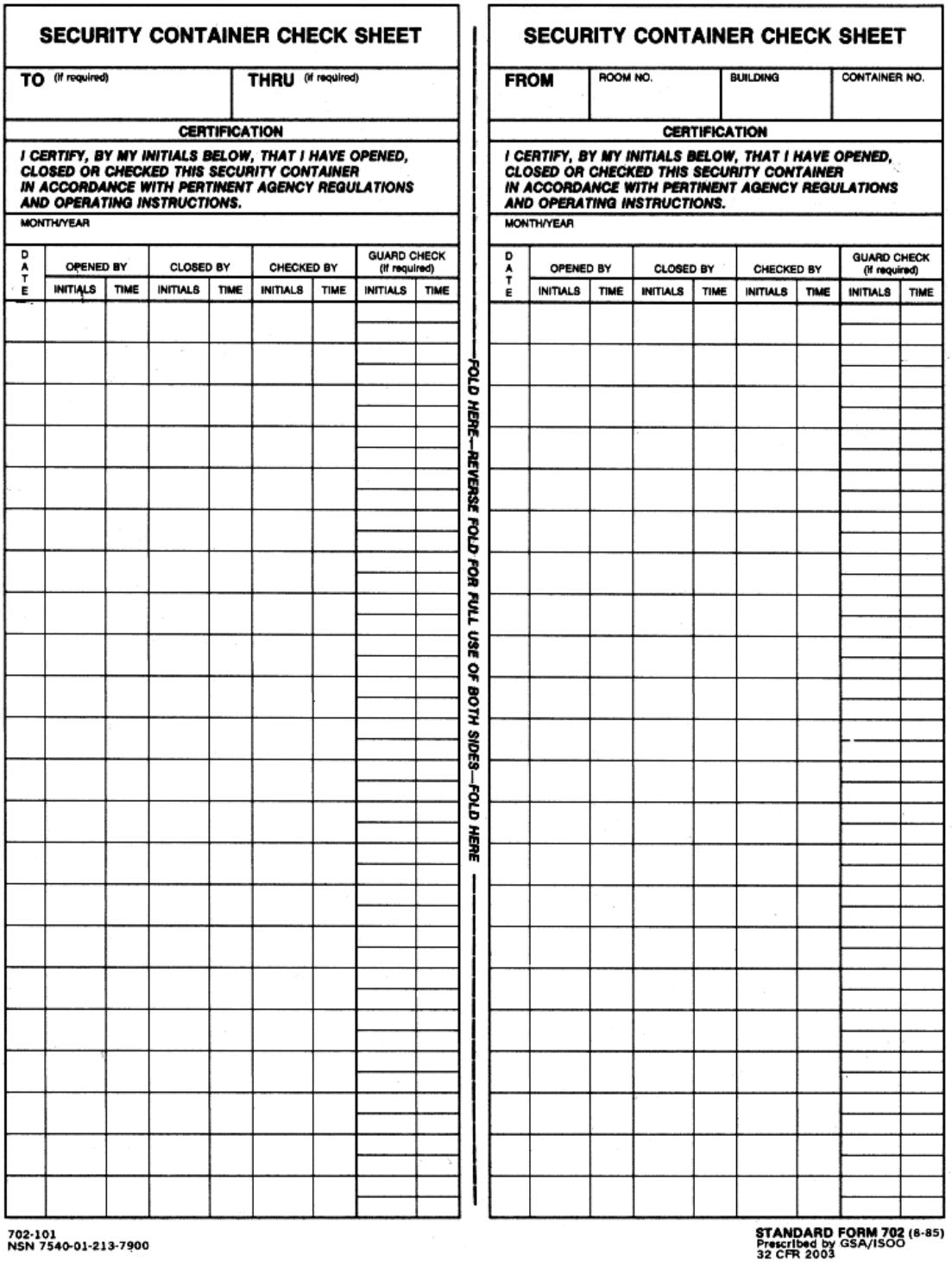
Privacy Act Statement

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.

Reverse Side

Note: When the SF 700 is reissued, all references to 12356 will be updated to reflect E.O. 12958.

Exhibit 5 Standard Form 702, "Security Container Check Sheet"



SECURITY CONTAINER CHECK SHEET

TO (If required) | THRU (If required)

CERTIFICATION

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

MONTH/YEAR

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

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

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

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

MONTH/YEAR

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

702-101
NSN 7540-01-213-7900

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

Exhibit 6 Required Sign for Property Covered Under 10 CFR Part 160

NO TRESPASSING
BY ORDER OF
THE UNITED STATES
NUCLEAR REGULATORY COMMISSION

The unauthorized entry upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Nuclear Regulatory Commission that has been designated as subject to the provisions contained in Part 160 of the rules and regulations of the Nuclear Regulatory Commission (10 CFR Part 160) is prohibited, and the unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon such facility, installation, or real property is prohibited.

Whoever willfully violates the aforesaid regulation of the Nuclear Regulatory Commission shall, upon conviction thereof, be punishable by a fine as specified in 10 CFR Part 160. Whoever willfully violates this regulation with respect to any facility, installation, or real property enclosed by a fence, wall, floor, roof, or other structural barrier shall be guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not to exceed $5,000 or imprisonment for not more than 1 year, or both.

By authority of Section 229 of the Atomic Energy Act of 1954, as amended, and Part 160 of the rules and regulations of the Nuclear Regulatory Commission, this facility, installation, or real property has been designated as subject to these regulations by the Nuclear Regulatory Commission.