FOIA/PA NO: 2016-0195

RECORDS ALREADY PUBLICLY AVAILABLE

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

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.