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

MD 12.4	**NRC COMMUNICATIONS SECURITY (COMSEC) PROGRAM**	**DT-17-228**
Volume 12:	Security	
Approved By:	Stephen G. Burns, Chairman	
Date Approved:	April 8, 2016	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Nuclear Security and Incident Response Division of Security Operations	
Contact Name:	Samuel Bazian 301-415-1504	Curtis Newkirk 301-415-0577

EXECUTIVE SUMMARY

Directive and Handbook 12.4, “NRC Communications Security (COMSEC) Program,” are being retitled and revised to clarify the agency’s roles and responsibilities for communications security (COMSEC) materials in accordance with Committee on National Security Systems (CNSS) Policy No. 1, “National Policy for Safeguarding and Control of COMSEC Materials.” CNSS Policy No. 1 replaces Handbook 12.4.

The policy and procedures for the physical security requirements and classified telecommunication systems are being transitioned into the appropriate management directives (MDs):

- MD 12.1, “NRC Facility Security Program,” currently provides the physical security requirements for a secure NRC telecommunications facility, as described in Section II, “Physical Security Requirements for the Protection of Classified Information,” of the handbook.
- MD 12.5, “NRC Cybersecurity Program,” will provide the requirements for the NRC telecommunications systems security program for classified telecommunication.

Accordingly, MD 12.4 is being retitled from “NRC Telecommunications Systems Security Program” to “NRC Communications Security (COMSEC) Program” to clarify the intent and the objectives of the COMSEC program.

For updates or revisions to policies contained in this MD that were issued after the MD was signed, please see the Yellow Announcement to Management Directive index (YA-to-MD index).

TABLE OF CONTENTS

I. POLICY

It is the policy of the U.S. Nuclear Regulatory Commission (NRC) that all classified or sensitive unclassified information transmitted on telecommunications systems that are under the security jurisdiction of the NRC be protected as required by law. Specifically, the NRC will ensure the safeguard and control of communications security (COMSEC) materials in a manner which assures their continued integrity, prevents access by unauthorized persons, and controls the spread of COMSEC materials, techniques, and technology.

II. OBJECTIVES

- Align with national COMSEC policy in accordance with the Committee on National Security Systems (CNSS) Policy No. 1, "National Policy for Safeguarding and Control of COMSEC Materials," dated September 2004.
- Establish a centralized COMSEC Material Control System for the agency, into which all COMSEC keying material will be placed.
- Safeguard the following information that is communicated on telecommunications systems:
  - National Security Information; and
  - Restricted Data and Formerly Restricted Data.
- Safeguard classified information communicated over telecommunications systems that prepare, transmit, communicate, or process the information (writing, images, sounds, or other data) by electric, electromagnetic, electromechanical, electro-optical, or other electronic means, using media to include twisted pair cable, coaxial cable, fiber optic cable, microwave, radio frequency, infrared, or satellite. These telecommunications systems include, but are not limited to, the following:
  - Telephones (wired and cellular);
  - Facsimiles;
  - Radios;
  - Video and video-teleconferencing systems;
  - Networks (wired and wireless); and
  - Other data transmission systems.
- Safeguard and control COMSEC in a manner that assures the continued integrity, prevents access by unauthorized persons, and controls the spread of COMSEC materials, techniques, and technologies.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Chairman

1. Ensures that the agency has implemented a COMSEC program that aligns with CNSS Policy No. 1.
2. Assumes ultimate management responsibility for the agency.

B. Executive Director for Operations (EDO)

1. Ensures the NRC complies with the national COMSEC policy requirements.
2. Designates collectively the Chief Information Officer (CIO); the Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital Programs (DEDM); and the Deputy Executive Director for Reactor and Preparedness Programs (DEDR) as the NRC's Designated Approving Authority (DAA) for major information technology (IT) investments, to include local accreditation of COMSEC accounting systems.[1]

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

1. Ensures a Central Office of Record (COR) is assigned as the NRC representative to the National Security Agency (NSA) for all matters relating to COMSEC.
2. Ensures that the office maintains the primary COR account and manages the subordinate COMSEC accounts.
3. Ensures that the COR meets reporting requirements to the NSA.
4. Ensures that the office has a qualified and trained COMSEC manager, a minimum of one alternate COMSEC manager, a COR, and an alternate COR.
5. Ensures COMSEC materials are available to carry out the program.
6. Ensures oversight of and is fully responsible for the NRC COMSEC program through COR functions.
7. Ensures subject matter experts are assigned for cryptographic equipment. Ensures that cryptographic requirements are determined including, specifications for acquisition and implementation of COMSEC materials and Controlled Cryptographic Items (CCI).
8. Ensures that all security incidents involving COMSEC materials, CCI, and facilities housing COMSEC materials and CCI are reported to the NSA and to the NRC Office of Administration.
9. Ensures users of COMSEC materials are properly trained before being granted access.

[1] See Section III.F in MD 12.5, "NRC Cybersecurity Program," for the responsibilities of the Designated Approving Authority (DAA). Additional information on DAA responsibilities for information technology investments (both major and non-major) are available on the Web site of the Office of the Chief Information Officer, Information Security Directorate, at http://www.internal.nrc.gov/CSO/DAA.html.

D. Director, Office of Administration (ADM)

1. Ensures physical security requirements are met and maintained for the protection of COMSEC materials and CCI.
2. Reports all security incidents involving COMSEC materials, CCI, and facilities housing COMSEC materials and CCI to the NRC COR.
3. Ensures personnel handling COMSEC materials or CCI have the proper security clearance.

E. Regional Administrators

1. Ensures the regional office maintains a COMSEC program subordinate to the COMSEC program at headquarters.
2. Ensures that the regional office has a qualified and trained COMSEC manager and a minimum of one alternate COMSEC manager.

F. Director, Information Security Directorate (ISD), Office of the Chief Information Officer (OCIO)

1. Administers NRC's internal Cybersecurity Program.
2. Keeps the NRC apprised of current cybersecurity threats, vulnerabilities, and mitigation measures.
3. Plans, directs, and oversees the implementation of the agencywide Cybersecurity Program, to include the electronic processing of classified information.

IV. APPLICABILITY

The policy and guidance in this directive and handbook apply to all NRC employees, contractors, and consultants.

V. DIRECTIVE HANDBOOK

A. Revised Handbook 12.4

Handbook 12.4 consists of the "National Policy for Safeguarding and Control of Communications Security Material" published by the Committee on National Security Systems (CNSS) in 2004. It summarizes the laws, regulations, and policies governing the safeguarding and control of COMSEC materials by all Federal employees. Its intent is to provide the roles and responsibilities for Federal agencies. CNSS Policy No. 1, "National Policy for Safeguarding and Control of Communications Security Material," is available at http://www.cnss.gov.

B. Procedures and Guidelines for Telecommunications System Security Program

1. Procedures and guidelines for implementation of the telecommunications systems security program may be found as follows:

   (a) Facility Requirements: MD 12.1, Handbook Section II;

   (b) Transmission and Emission Security: MD 12.5, NRC Cybersecurity Program Handbook Section VI; and

   (c) Secure Telecommunications Systems: MD 12.5, NRC Cybersecurity Program Handbook Section VI.

2. Please note that CNSS Policy No. 1 addresses facility operations and that MD 12.2, “NRC Classified Information Security Program,” addresses the handling of classified information.

VI. NRC COMMUNICATIONS SECURITY PROGRAM

A. General

The NRC COMSEC program is governed by CNSS, as well as other Federal agencies and external drivers. The committee is comprised of voting members from 21 United States Government Executive Branch departments and agencies. In addition, there are 14 official Committee Observers representing additional organizations outside of the Executive Branch, of which the NRC is one. The Committee carries out the work of protecting the National Security Systems by developing operating policies, procedures, guidelines, directives, instructions, and standards as necessary to implement National Security Directive (NSD) 42, “National Policy on the Security of National Security Telecommunications and Information Systems,” July 5, 1990.

B. Federal Requirement to Implement the Policies and Directives of the Committee on National Security Systems

CNSS issuances are directed at those entities that own and/or are users of national security systems. The heads of the executive departments and agencies are responsible for ensuring that CNSS policies and directives are implemented within their departments or agencies. As a user of national security systems, the NRC is required to implement the policies and directives issued by CNSS.

C. Transmission of Classified Information

All routine electronic transmissions of classified information must be transmitted using technologies in accordance with YA-14-130 and MD 12.5. See also MD 12.2 for the policy and procedures to protect and control classified information.

VII. REFERENCES

Executive Orders

Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001.

Executive Order 13284, "Amendment of Executive Orders and Other Actions, in Connection with the Establishment of the Department of Homeland Security," January 23, 2003.

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

National Security Policy and Memoranda

Committee on National Security Systems (CNSS) Policy No. 1, "National Policy for Safeguarding and Control of Communications Security Material," September 2004.

National Security Agency Central Security Service (NSA/CSS) Policy Manual No. 3-16, "Control of Communications Security (COMSEC) Material," August 2005.

National Security Directive (NSD) 42, "National Policy on the Security of National Security Telecommunications and Information Systems," July 5, 1990.

Nuclear Regulatory Commission

NRC Management Directives—

3.2, "Privacy Act."

12.1, "NRC Facility Security Program."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.5, "NRC Cybersecurity Program."

NRC Web Sites

Designated Approving Authorities for Major and Non-Major IT Investments, OCIO/ISD Web Site: http://www.internal.nrc.gov/CSO/DAA.html.

NSIR Information Security Branch (NSIR/DSO/ISB) Web Site: http://nsir.nrc.gov/securityoperations/infosecurity.aspx.

NRC Security Web Site:
http://www.internal.nrc.gov/security.html.

United States Code

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

Energy Policy Act of 2005, Pub. L. 109-58.