U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT–99–31

To:	NRC Management Directives Custodians
Subject:	Transmittal of Directive 12.4, "NRC Telecommunications Systems Security Program"
Purpose:	Directive and Handbook 12.4 have been revised to reflect changes in organizational responsibilities and delegations of authority for the Chief Information Officer and the Division of Facilities and Security, Office of Administration (ADM). ADM will assume primary responsibility for NRC secure telecommunications programs, including planning, budgeting, and support. This change also removes two examples of protected telephone systems that are no longer valid.
Office and Division of Origin:	Office of Administration
Contact:	Nancy Fontaine, 301–415–1253
Date Approved:	January 21, 1998 (Revised: December 8, 1999)
Volume:	12 Security
Directive:	12.4 NRC Telecommunications Systems Security Program
Availability:	Rules and Directives Branch Office of Administration David L. Meyer (301)415–7162 or Jeannette P. Kiminas (301)415–7086

NRC Telecommunications Systems Security Program

Directive 12.4

Contents

NRC Telecommunications Systems Security Program Directive 12.4

Policy
(12.4–01)

It is the policy of the U.S. Nuclear Regulatory Commission 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.

Objectives
(12.4–02)

- To safeguard the following information that is communicated on telecommunications systems. (021)
  - National Security Information (a)
  - Restricted Data and formerly Restricted Data (b)
  - Sensitive unclassified information (c)
    - Privacy information (i)
    - Proprietary Information (ii)
    - Safeguards Information (iii)
  - Other sensitive information as defined by the Computer Security Act of 1987 (d)
- To safeguard classified or sensitive unclassified information communicated over telecommunications systems that prepare, transmit, communicate, or process the information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means, using

Objectives
(12.4–02) (continued)

media such as twisted pair cable, coaxial cable, fiber optic cable, microwave, or satellite. These telecommunications systems include, but are not limited to, the following: (022)

- Telephones (a)
- Facsimiles (b)
- Radios (c)
- Video and video-teleconferencing systems (d)
- Networks (i.e., local area network and wide area network) (e)
- Other data transmission systems (f)

Organizational Responsibilities and Delegations of Authority
(12.4–03)

Deputy Executive Director for Management Services (DEDM)
(031)

- Acts as the Senior Agency Official for issues involving classified information. (a)
- Authorizes, directly or by designee, exceptions to or deviations from this directive within the limitations of authority set by law and Federal regulation. (b)

Chief Information Officer (CIO)
(032)

- Reviews and approves, in conjunction with the Division of Facilities and Security (DFS), Office of Administration, security proposals and plans originated by NRC offices, licensees, certificate holders, and contractors, for telecommunications systems, facilities, and communication centers to be used for communicating classified or sensitive unclassified information. (a)

Chief Information Officer (CIO)
(032) (continued)

- Reviews and concurs in feasibility studies for requested new NRC telecommunications systems that will communicate classified or sensitive unclassified information. (b)
- Reviews information copies of facility security surveys conducted by DFS on non-network systems that handle classified or sensitive unclassified information; acts on specific recommendations in accordance with Handbook 12.4. (c)
- Provides engineering design services for all cryptographic and related terminal equipment that interfaces with common carrier circuitry; orders the installation of this equipment. (d)
- Reviews, comments, and concurs in documents of the National Security Telecommunications and Information Systems Security Committee (NSTISSC). (e)
- Appoints an observer to the Subcommittee on Information Systems Security. (f)
- Provides technical support and installation of high-speed data lines, as needed. (g)

Office Directors and Regional Administrators
(033)

- Specify, budget, order, install, move, test, and maintain telecommunication systems under their jurisdiction and arranges for appropriate training of personnel. (a)
- Ensure that all secure telecommunications systems operated by NRC or NRC contractors comply with this directive and handbook to safeguard classified or sensitive unclassified information. (b)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(034)

- Ensures that classified or sensitive unclassified information processed by systems used by NRC headquarters and regional offices is safeguarded. (a)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(034) (continued)

- Reviews and approves NRC security proposals and plans, contracts, and interagency agreements involving classified or sensitive unclassified information; conducts feasibility studies and issues security requirements for systems that communicate classified or sensitive unclassified information. (b)
- Conducts system security surveys and provides followup recommendations to ensure compliance with security policies for non-network systems that handle classified or sensitive unclassified information. (c)
- Serves as the observer to NSTISSC and observer to the NSTISSC Subcommittee on Telecommunications Security. (d)
- Serves as the NRC representative to the National Security Agency for all matters relating to communications security (COMSEC), such as COMSEC accounting, COMSEC training, and the Central Office of Record. (e)
- Serves as the Command Authority for the secure telephone unit and secure terminal equipment; appoints user representatives for NRC and specifies key ordering privileges. (f)
- Manages and operates the Secure Communications Center, including budgeting, ordering, installing, moving, testing, and maintaining telecommunications systems. (g)
- Specifies, budgets, orders, installs, moves, tests, and maintains agency infrastructure components, including NRC headquarters telecommunications systems that communicate classified or sensitive unclassified information; trains or arranges training for personnel on these systems; originates statements of work, work orders, and requests for procurement action. (h)
- Approves all purchase requests from NRC regions for telecommunications systems that transmit classified or sensitive unclassified information. (i)
- Coordinates services performed by the General Services Administration or other contractors, including issuing necessary budget documents and work orders for cryptographic, red/black wiring, and installation for telecommunications systems that process classified information. (j)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(034) (continued)

- Ensures, through proper coordination with the Personnel Security Branch, that all individuals designated to participate in the design, planning, operation, or maintenance of NRC telecommunications systems, or centers that communicate classified or sensitive unclassified information, are properly screened and eligible for access to this information or these systems before this access is granted. (k)
- Ensures the adequacy of the security requirements included in contracts, interagency agreements, and designs for NRC telecommunications systems that handle classified or sensitive unclassified information. (l)
- Determines requirements for cryptographic equipment and defines specifications for the acquisition and implementation of automated information equipment or systems that process or produce classified or sensitive unclassified information. (m)
- Ensures that any construction, expansion, or restack of NRC areas or facilities having or requiring telecommunications systems, is coordinated with Office of the CIO (OCIO) during both planning and installation phases. (n)

Director, Division of Contracts and Property Management (DCPM), ADM
(035)

- Ensures that all Federal and NRC requirements for the protection of classified or sensitive unclassified information are provided in solicitations and contracts. (a)
- Ensures that redistribution, destruction, and disposal of NRC telecommunications systems that have been used to process classified or sensitive unclassified information, is coordinated through OCIO and DFS before release. (b)

Associate Director for Training and Development, Office of Human Resources (HR)
(036)

- Assists in the development and delivery of appropriate security training programs for NRC personnel who work on NRC telecommunications systems, as requested. (a)

Associate Director for Training and Development, Office of Human Resources (HR)
(036) (continued)

- Provides other security-related training, as requested. (b)
- Ensures the inclusion of a security briefing in the initial orientation of new employees. (c)

Applicability
(12.4–04)

The policy and guidance in this directive and handbook apply to all NRC employees, consultants, experts, panel members, contractors, and subcontractors who transmit classified or sensitive unclassified information on telecommunications systems that are under the jurisdiction of NRC, including those performing work for the NRC pursuant to interagency agreements, memoranda of understanding, or financial assistance programs. This directive does not apply to NRC licensees or certificate holders.

Handbook
(12.4–05)

Procedures and guidelines for implementation of the telecommunications systems security program are contained in Handbook 12.4.

References
(12.4–06)

Computer Security Act of 1987, Pub. L. 100-235.

Management Directive 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 Automated Information Systems Security Program."

— 12.6, "NRC Sensitive Unclassified Information Security Program."

References
(12.4–06) (continued)

National Security Agency (NSA),* Electronic Key Management System (EKMS) 702.01, "STU-III Key Management Plan," and supplements.

—, Manual 90-2, "COMSEC Material and Control Manual."

National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security."

National Security Telecommunications and Information Systems Security (NSTISSI),** No. 4001, "Controlled Cryptographic Items."

—, No. 4005, "Safeguarding COMSEC Facilities and Material."

Office of Management and Budget Circular A-130, "Management of Federal Information Resources."

National Security Telecommunications and Information Systems Security Advisory Memorandum TEMPEST 2-95, "Guidelines for Facility Design and Red/Black Installation," dated November 1, 1995.

* Copies of NSA documents are available to all NRC personnel assigned COMSEC responsibilities, or upon written request to the Director, DFS.

** Contact the Chief, INFOSEC, for a copy of NSTISSI documents.

NRC Telecommunications Systems Security Program

Handbook 12.4

Contents

Contents (continued)

Part II (continued)

Exhibit

Part I
Introduction

This handbook contains the procedures for planning, implementing, maintaining, and monitoring the security of NRC contractor and NRC telecommunications systems that communicate classified and sensitive unclassified information. It does not address traditional computer security or physical security issues except when they are directly related to the protection of information during processing or transmission. This handbook is intended for use in combination with other management directives and handbooks, and in conjunction with National Security Telecommunications and Information Systems Security (NSTISS) publications, National Security Agency (NSA) Communications Security (COMSEC) publications, and NRC policies. (A)

A list of the Federal authorities involved with telecommunications systems security is given below. (B)

- **National Security Council/Policy Coordinating Committee (NSC/PCC) for National Security Telecommunications and Information Systems (1)**

  This committee consists of the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Energy, the Secretary of Commerce, the Director of Central Intelligence, the Assistant Director for National Security Affairs, the Director of the Office of Management and Budget, the Senior Director for Defense Policy and Arms Policy of the NSC, and is chaired by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The National Manager for NSTISS participates as an observer.

- **The National Security Telecommunications and Information Systems Security Committee (NSTISSC) (2)**

  This committee is established to operate under the guidance of the NSC/PCC for National Security Telecommunications and

Information Systems to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement the provisions of the directive entitled "National Policy for the Security of National Security Telecommunications and Information Systems." The NRC is a non-voting member of this committee.

- **Executive Agent of the Government for National Security Telecommunications and Information Systems Security (3)**

  The Secretary of Defense is the Executive Agent of the Government for NSTISS and is responsible for implementing, under his signature, the policies developed by the NSTISSC.

- **National Manager for National Security Telecommunications and Information Systems Security (4)**

  The Director, NSA, is designated the National Manager for NSTISS. The NSA prescribes or approves all cryptographic systems and techniques used by or on behalf of the U.S. Government. These responsibilities include, but are not limited to:

  - Conducting, approving, or endorsing research and development of techniques and equipment to secure national security systems (a)
  - Reviewing and approving all standards, techniques, systems, and equipment related to the security of national security systems (b)
  - Prescribing the minimum standards, methods, and procedures for protecting cryptographic and other technical security material, techniques, and information related to national security systems (c)

Part II
Security of Telecommunications

Communications Security (COMSEC) (A)

General (1)

Communications security is the protection of information while it is being transmitted by telephone, cable, microwave, satellite, or any other means. It includes cryptographic security, transmission security, emission security, and physical security of COMSEC material. COMSEC is a program that certifies cryptographic and other communications security products.

Sensitivity of COMSEC Information (2)

COMSEC information is considered especially sensitive because of the need to safeguard U.S. cryptographic principles, methods, and material against exploitation.

COMSEC Material and Equipment (3)

COMSEC material and equipment are items designed to secure or authenticate telecommunications. This includes, but is not limited to, keys, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic or performs COMSEC functions. Information and material that are designated and marked are made available only to appropriately cleared personnel who have a legitimate need-to-know. COMSEC material and equipment are issued to and transferred only between COMSEC accounts. If further distribution is required, COMSEC custodians or alternates will issue the material or equipment on temporary "hand receipts." Hand receipts must be reissued every 6 months by the COMSEC custodian.

Communications Security (COMSEC) (A) (continued)

Control of COMSEC Material (4)

NRC COMSEC material will be controlled in accordance with current National Security Telecommunications and Information Systems Security (NSTISS) directives. COMSEC material consists of aids, equipment, components, and devices that are identifiable by the National Security Agency (NSA) telecommunications security nomenclature system. (a)

The NRC follows the NSA COMSEC accounting policies and procedures as prescribed in NSA Manual 90-2, "COMSEC Material and Control Manual," and Electronic Key Management System (EKMS) 702.01, "STU-III Key Management Plan." Copies of the above manuals are available to all NRC personnel assigned COMSEC responsibilities, or upon written request to the Director, DFS. (b)

Controlled Cryptographic Items (CCI) (5)

Controlled cryptographic items are secure telecommunications or information handling equipment or associated cryptographic components that are unclassified but governed by a special set of control requirements determined by the NSA. These items are marked "Controlled Cryptographic Item," or "CCI." CCI items are accounted for and controlled through the NSA COMSEC material control system (CMCS).

Other Materials (6)

Materials such as COMSEC instructional documents, COMSEC equipment operating and maintenance manuals, cryptographic ancillary material, are not cryptographic in scope, and are not marked "CRYPTO" or subject to the special safeguards required for information bearing that marking. However, for logistical control purposes, and as an identification aid to communications personnel, "non-crypto" COMSEC materials essential to secure communications are issued and transferred through the CMCS and made available only on a need-to-know basis. (a)

Communications Security (COMSEC) (A) (continued)

Other Materials (6) (continued)

Materials such as correspondence, messages, or publications, that are related to secure communications operations, but do not contain cryptographic information, are handled in accordance with the material classification or marking. Generally, all materials that mention or describe NRC secure communications facilities, operations, or capabilities, or that use short title designations of COMSEC material, require the minimum designation of "Official Use Only." (b)

Access to Cryptographic and COMSEC Information (7)

Certain U.S. classified cryptographic and/or COMSEC information, the loss of which could cause serious or exceptionally grave damage to U.S. national security, requires special access controls. An individual may be granted access to U.S. classified cryptographic information or COMSEC information, only if that individual—

- Is a U.S. citizen (a)
- Is an employee of the U.S. Government, is a U.S. Government-cleared contractor or employee of such contractor, licensee, certificate holder, or is employed as a U.S. Government representative (including consultants of the U.S. Government) (b)
- Possesses a security clearance appropriate to the classification level of the U.S. cryptographic information or COMSEC information to be accessed (c)
- Possesses a valid need-to-know as determined necessary to perform duties for, or on behalf of, the U.S. Government (d)
- Receives a security briefing appropriate to the U.S. cryptographic information or COMSEC information to be accessed (e)
- Acknowledges the granting of access by signing a cryptographic access or COMSEC access certificate (f)

Communications Security (COMSEC) (A) (continued)

NRC Contractor COMSEC Authorizations (8)

Managers shall obtain Division of Facilities and Security (DFS), Office of Administration, authorization for either—(a)

- The release of operational COMSEC material to contractors, licensees, or certificate holders, for the purpose of transmitting classified information or data (i)
- The use of contractor personnel to install, maintain, or operate a secure communications facility for NRC (ii)

Managers also shall advise DFS of the start and termination of the actual use of such authorizations. (b)

COMSEC Functional Designations and Responsibilities (9)

COMSEC Control Officer (a)

The Chief, Information Security Branch (INFOSEC), DFS, is the COMSEC Control Officer for the agency and is responsible for the operation of the NRC Central Office of Record (COR) and for specifying control criteria for all COMSEC material.

Central Office of Record (b)

COR performs oversight of all NRC COMSEC accounts. COR coordinates all COMSEC activities with the National Security Agency (NSA) for NRC, particularly the accounting of all COMSEC material. (i)

COR periodically inspects all NRC COMSEC accounts. The Director, DFS, will send the cognizant organization any deficiency reports resulting from the inspection. The cognizant organization is responsible for correcting any deficiencies, just as it would implement recommendations from other security surveys or inspections. (ii)

The requirement to audit the NRC COR is vested in the NSA. NSA conducts these audits periodically and directs any resulting deficiency reports to the Director, DFS, for correction. NSA may audit individual COMSEC accounts at any time and provide resulting audit reports to the individual COMSEC accounts, with copies of deficiency reports to COR. (iii)

Communications Security (COMSEC) (A) (continued)

COMSEC Functional Designations and Responsibilities (9) (continued)

STU-III Command Authority (c)

The STU-III Command Authority is responsible for appointing, adding, deleting, or making changes to information regarding user representatives and their key ordering privileges. In most cases, user representatives are COMSEC custodians and alternates who order STU-III keying material for the secure telephones.

COMSEC Custodian (d)

The NRC currently has five COMSEC accounts, located at headquarters and each regional office. Each account has a primary custodian and 1 to 2 alternate custodians. COMSEC custodian duties include the receipt, transfer, accounting, safeguarding, and destruction of all COMSEC material assigned to the custodian's specific account. Managers shall nominate candidates in writing to the Director, DFS, and provide the individual's name, social security number (SSN), date of birth, place of birth, and security clearance or access authorization. COMSEC custodians must possess a "Q" clearance. The COR, after verification of clearance information, will appoint the COMSEC custodian in writing. Managers and candidates should be aware that there is a mandatory requirement for formal COMSEC custodian training upon assumption of COMSEC duties. When a change in custodian becomes necessary, the responsible manager shall submit a request for the change to the NRC COR at least 45 days in advance of the departure of the COMSEC custodian to allow for a change-of-custodian inventory to be conducted. If this is not possible, contact the COR for direction.

Alternate COMSEC Custodian (e)

Alternate COMSEC custodians assist the COMSEC custodian in the duties listed above. During periods when the COMSEC custodian is unavailable, the alternate custodian is authorized to perform these duties. Managers shall nominate candidates in writing to the Director, DFS and provide the individual's name, SSN, date of birth, place of birth, and clearance access level. Alternate COMSEC custodians must possess a "Q" clearance. The COR, after verification of clearance

Communications Security (COMSEC) (A) (continued)

COMSEC Functional Designations and Responsibilities (9) (continued)

information, will appoint the Alternate COMSEC custodian in writing. Managers and candidates should be aware that there is a mandatory requirement for formal COMSEC custodian training upon assumption of COMSEC duties.

Users (f)

The individual user or holder of COMSEC material is personally responsible for the control and safeguarding of COMSEC material while it is entrusted to his or her care.

Installation of COMSEC Equipment (10)

Installation of Government-owned COMSEC equipment is subject to policies established by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and procedures set forth for the type of equipment involved. COMSEC equipment shall not be installed for new applications until all the following requirements have been met:

- Approved storage containers for the appropriate level of classified COMSEC material have been provided (a)
- The installation has been afforded the required physical safeguards and access controls (b)
- A security plan has been approved by Director, DFS (c)

Acquisition of COMSEC Material (11)

All accountable COMSEC material, with the exception of the keying material for the secure telephone unit-generation three (STU-III), shall be controlled through the COMSEC CMCS. STU-III keying material shall be controlled through the NSA key management system (KMS). Contact your COMSEC custodian or the NRC COR to obtain both COMSEC material and STU-III keying material.

Communications Security (COMSEC) (A) (continued)

Releasing COMSEC Information to U.S. Contractors and Other Sources Outside the U.S. Government (12)

It should be noted that the release of COMSEC and COMSEC-related information, such as National Security Telecommunications and Information Systems Security Instructions (NTISSI) and National Communications Security Instructions (NACSI), to U.S. contractors and other U.S. non-governmental personnel is generally restricted. Any release of NRC COMSEC material to U.S. contractors and other U.S. non-governmental sources must be approved in advance by the Director, DFS.

Reporting COMSEC Insecurities (Incidents) (13)

The immediate reporting of any incident that may have subjected accountable classified COMSEC information furnished to NRC COMSEC accounts to be compromised is essential to ensuring the continued integrity of the information itself and the communications media protecting the information. In almost all cases, timely reporting of compromises to DFS will minimize the effects of the violation or loss of the information. The longer the delay in reporting incidents of security interest, the more difficult it becomes to determine and minimize the effect on national security. (a)

In reporting possible compromises to DFS and the NRC COR, the preferred mode of transmission is the STU-III, or successor equipment. When secure communications are not available, an unclassified report giving a brief unclassified description of the incident should be provided to DFS within 12 hours after discovery. After normal duty hours and on weekends and holidays, unclassified reports should be made to the Director, DFS, or the Chief, INFOSEC, through the NRC operator on 301-415-7000. (b)

In all cases, telephonic reports will be followed up by written correspondence, classified if appropriate, to Director, DFS, and, if accountable, COMSEC material is involved, also to the NRC COR. A followup written report detailing initial investigative actions and results should be submitted within 72 hours, and a final written report should be submitted within 30 days. Complete details of the incident and investigation are essential to determining the impact and followup actions necessary to minimize the effects of a compromise or security

Communications Security (COMSEC) (A) (continued)

Reporting COMSEC Insecurities (Incidents) (13) (continued)

violation and to draw a reasonable conclusion on the basis of fact. Each written report of a security incident involving COMSEC information should contain, as a minimum—(c)

- Name and address of the COMSEC account (i)
- Designated COMSEC custodian for the COMSEC account and the custodian's telephone number (ii)
- COMSEC account number (iii)
- Identification of the material involved (iv)
- Type of area control in effect (v)
- Description of the incident (vi)
- Personnel involved and their clearance levels (vii)
- Results of material inventory (viii)
- Investigative actions initiated and preliminary results (ix)
- Evaluation by the action officer of whether a compromise occurred (x)
- Actions taken to prevent recurrence of the incident (xi)

Followup and final reports will be classified a minimum of "CONFIDENTIAL-NSI" and should be marked "DECLASSIFY on: X1."

COMSEC Emergency Procedures (14)

Each organization holding classified or CCI COMSEC material must maintain a current, written emergency plan for the protection of this material during emergencies. NSTISSI 4004, "Routine Destruction and Emergency Protection of COMSEC Material," dated March 11, 1987, or successor editions, provides guidance and information. Contact the COR to obtain a copy of the current document, or if additional information is required. These plans should be included in standard operating procedures and also should be posted as a separate document where it can be referenced by personnel during an emergency situation. The COMSEC emergency plans are approved by the COR and reviewed during COMSEC audits.

Secure Telecommunications Facilities Requirements (B)

Safeguarding COMSEC Facilities (1)

NRC-approved COMSEC facilities used for communicating National Security Information or Restricted Data shall be safeguarded in accordance with NSTISS directives. (a)

Cleared NRC personnel having a need-to-know, primarily as a result of their involvement in the supervision of the design, construction, or operation of an NRC COMSEC facility, may obtain copies of the applicable NSTISS directives upon written request to the Director, DFS. (b)

Establishment of a Secure Telecommunications Facility (2)

The feasibility and advisability of a secure telecommunications facility should first be established by preliminary communications with DFS. Once established, the NRC office requesting the telecommunications facility submits to DFS, for evaluation and approval, a security proposal for the facility, using the format provided in the exhibit of this handbook. Refer to NSTISSI 4005, "Safeguarding COMSEC Facilities and Material," for minimum requirements for the construction and safeguarding of secure telecommunications facilities. Contact the Chief, INFOSEC, for a copy of this document. (a)

The proposal shall be developed only if a strong requirement exists for such a facility. Limitations on the number of secure facilities and the concentration of security measures at a centralized location is usually more prudent than creating multiple facilities. (b)

For NRC offices, OCIO and DFS will provide certain essential information for the proposal upon request, for example, floor plans, cryptographic equipment selections, and alarm designs. (c)

In each proposal, more detailed technical information may have to be elicited from the requesting office regarding the communicating techniques to be used. (d)

Secure Telecommunications Facilities Requirements (B) (continued)

Establishment of a Secure Telecommunications Facility (2) (continued)

When the security proposal is approved, it will become the facility communications security plan. It must be updated by the COMSEC Control Officer when modifications to the facility are proposed and must be resubmitted through the same process for approval. Copies of the plan, sound attenuation test reports, technical surveillance countermeasures (TSCM) reports, inspection reports, and TEMPEST test results, when required by NRC or other agencies, will be kept on file in DFS. (e)

Classified information may be discussed or transmitted only over those secure systems the Director, DFS, has approved in writing. (f)

If more than one type of telecommunications system is desired for a single communications center, the user organization must submit only one proposal to the OCIO. If a telecommunications center also is to include the telecommunication of data from automated information systems (AIS), the proposal should be written to cover all systems. Both DFS and OCIO are involved in the development of the proposal and the approval process for NRC users. See the guidelines for security proposals for AIS systems contained in Management Directive (MD) 12.5, "NRC Automated Information Systems Security Program." (g)

Security Clearance for Installation, Maintenance, and Modification (3)

The installation, maintenance, and modification of a secure communications facility presents an opportunity for hostile penetration that may not be present when an encrypted signal is used. Ideally, all maintenance personnel should possess a final government issued security clearance. Personnel without a final security clearance may be used, but must be under constant visual observation by technically qualified and cleared NRC or NRC contractor personnel. A technical inspection must be conducted prior to the transmission of classified information. Uncleared persons must not have access to classified data transmitted via the system.

Secure Telecommunications Facilities Requirements (B) (continued)

Guidelines for Facility Design and Red/Black Installation (4)

Secure telecommunications systems must be installed in accordance with NSTISSAM TEMPEST 2-95, "Guidelines for Facility Design and Red/Black Installation," dated November 1, 1995. This document defines the guidance to consider during the design of facilities and for subsequent installation of equipment and systems that receive, transmit, manipulate, graph, store, archive, calculate, generate, print, or in any other manner, process national security information. Red/black installation recommendations, TEMPEST facility considerations, administrative support equipment (e.g., telephone systems, intercoms, alarms, and radio devices), cabling, inspectable space, and facility shielding are discussed in this document. Contact the Chief, INFOSEC, to obtain copies of this document.

Operation of Secure Telecommunications Facilities (C)

General Guidelines and Procedures (1)

There are numerous documents that provide guidance for the operation of secure telecommunications facilities from NSA and the NSTISSC. Contact the Chief, INFOSEC, to obtain copies of these documents.

Standard Operating Procedures (2)

The details for operating a telecommunications facility must be developed by the operating personnel under the direction of the COMSEC Control Officer on a case-by-case basis within the constraints imposed by the various NSA, NSTISSC, and NRC guidance documents.

Equipment Operation (3)

The operation of COMSEC equipment in NRC and NRC contractor systems must conform to NSA operations and maintenance manuals published for specific pieces of COMSEC equipment. Equipment that has been newly installed, relocated, or modified must not be operated until DFS has performed the required security checks of the operational

Operation of Secure Telecommunications Facilities (C) (continued)

Equipment Operation (3) (continued)

area. DFS-authorized qualified maintenance personnel also must check the equipment and determined that it is properly installed with all required modifications and ready for operation.

Handling of Information (4)

Classified and sensitive unclassified information shall be prepared, received, safeguarded, distributed, and disposed of in accordance with the requirements and procedures specified in MD 12.2, "NRC Classified Information Security Program," and MD 12.6, "NRC Sensitive Unclassified Information Security Program."

Security Surveys of Telecommunications Systems (5)

Telecommunications systems that receive, process, transmit, or safeguard classified data or information must be surveyed by DFS in accordance with the requirements and procedures of MD 12.1, "NRC Facility Security Program." The Director, DFS, shall furnish a statement of any proposed corrective actions resulting from the survey to the responsible headquarters office, division, regional office, or contractor. (a)

NRC COR inspections of all NRC COMSEC accounts will be performed periodically. The Director, DFS, will send the cognizant organization any deficiency reports resulting from the inspection for correction of the deficiency. The cognizant organization is responsible for correcting any deficiencies, just as it would implement recommendations from other security surveys or inspections. (b)

Followup of Deficiencies (6)

Managers shall ensure that their personnel follow up on any security deficiencies involving COMSEC or telecommunications systems. In turn, managers shall report any such matters to DFS, as required by this handbook.

Transmission and Emission Security (D)

Transmission Security (1)

Transmission security is the component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. To accomplish this, separation requirements are put into place to ensure classified information cannot be inadvertently transferred to unclassified transmission media and equipment. Red/black separation requirements and shielded cabling, along with the use of cryptographic equipment and technical surveillance countermeasures inspections at NRC, are the minimum recommended criteria for the design/installation of equipment within NRC controlled areas. Contact the Chief, INFOSEC, for additional information. (a)

Additional information regarding TSCM inspections can be found in MD 12.1. (b)

Administrative telephones, intercom systems, and public address systems shall not be placed within 3 feet, and telephone wires or unclassified data communication lines shall not be placed within 1 foot, of a microcomputer system processing classified information or attached to a classified network. Communication lines, telephones, and other equipment and connections, in adjoining rooms, ceilings, and floors also are considered for purposes of distance separation. If it is necessary to have a telephone, telephone wires, intercom, or an unclassified data communication line closer than the minimum distances, the Director, DFS, must approve this in writing. (c)

Emission Security (2)

Emissions security is the protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from cryptographic equipment or an information system. (a)

All electronic equipment (e.g., microcomputers, typewriters, printers, scanners) emit electrical and electromagnetic radiation through the air or through conductors. The possibility exists that electronic eavesdroppers could intercept emanations, decipher them, and use this information to reconstruct the data being processed by the equipment, even being located some distance from the equipment. The use of TEMPEST-certified technology is the preferred method of protecting against compromising emanations. (b)

Transmission and Emission Security (D) (continued)

TEMPEST (3)

TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment. (a)

Under certain circumstances and in some specific physical environments, non-TEMPEST telecommunications equipment may be used to communicate classified information when the Director, DFS, approves this in writing. (b)

Whether a specific piece of equipment can be used in certain cases in an unshielded environment must be determined on a case-by-case basis in the normal process of developing a security proposal. (c)

Technical Security Inspections (4)

DFS, will, upon request, arrange for technical security inspections such as TEMPEST and/or countermeasures inspections of secure telecommunications systems or facilities as dictated by local conditions or circumstances. (See MD 12.1 for additional information.)

Protection of Sensitive Unclassified Information (E)

Telecommunications Protection Authority (1)

The protection of sensitive unclassified information transmitted over telecommunications media (e.g., voice, video, network, facsimile, or other telecommunications systems) is required under National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security," and the Office of Management and Budget Circular A-130, "Management of Federal Information Resources." (a)

Protection of Sensitive Unclassified Information (E) (continued)

Telecommunications Protection Authority (1) (continued)

The procedures for the protection of sensitive unclassified information or data transmitted over telecommunications circuits used by any type of telecommunications system is given below. The general categories of sensitive unclassified that must be protected during NRC telecommunications transmissions are defined in MD 12.6, and include Proprietary, Official Use Only, and Safeguards Information (SGI). (b)

Telecommunications Protection Procedures (2)

Record Telecommunications (a)

Record telecommunications include the telecommunication of data and information using network automated information systems and facsimile equipment. Telecommunications security for automated information systems must meet the requirements of MD 12.5. (i)

Sensitive unclassified record telecommunications using automated information systems, laptops, and/or facsimile systems must be transmitted over protected systems. Examples of protected systems include the following: (ii)

- Unclassified systems that use hardware or software implementations of the data encryption standard (DES) that the Director, DFS, has approved in writing. *(a)*
- Unclassified systems that use hardware or software implementations of non-DES algorithms that the Director, DFS, has approved in writing. *(b)*
- Other unclassified systems that the Director, DFS, has approved in writing. *(c)*
- Secure classified systems that use encryption equipment certified by NSA for the transmission of National Security Information and Restricted Data. *(d)*

Protection of Sensitive Unclassified Information (E) (continued)

Telecommunications Protection Procedures (2) (continued)

Voice Telecommunications (b)

Sensitive unclassified voice telecommunications should be transmitted by protected systems to the maximum degree possible. The STU-III is the NRC-preferred telephone for the voice transmission of sensitive unclassified. Contact the Chief, INFOSEC, for the availability of STU-III telephones.

Privacy Act (c)

Managers shall ensure compliance with the provisions of MD 3.2, "Privacy Act," if the information communicated or contained in the system is subject to the Privacy Act of 1974, as amended.

Secure Telecommunications Systems at NRC (F)

General (1)

Managers of NRC or NRC contractor telecommunications systems that process classified and/or sensitive unclassified information must ensure that personnel having access to the system are cognizant of and comply with the provisions of this handbook.

Security Proposals and Plans (2)

Managers shall obtain prior approval from DFS and OCIO for the operation of any telecommunications system by means of security proposals and plans.

Review of Telecommunications Traffic (3)

In conjunction with OCIO, and when requested by DFS, managers shall review the categories or subjects of unsecured clear voice radio and telephone traffic under their jurisdiction to determine whether any systems pass traffic of significant intelligence value. Managers shall furnish the results of these reviews to DFS through OCIO. As necessary, managers shall request OCIO to provide secure COMSEC equipment or privacy equipment.

Secure Telecommunications Systems at NRC (F) (continued)

Record Telecommunications (4)

Secure Facsimile (a)

All classified and sensitive unclassified information telecommunicated via facsimile must be transmitted over protected systems. The DFS's Secure Communications Center (COMCtr) provides secure facsimile service for the NRC headquarters, utilizing STU-III telephones for encryption. The Secure COMCtr operates daily during normal working hours. For emergencies, the DFS also has procedures for the receipt or transmission of information outside of normal working hours. In addition to the COMCtr, AEOD's Emergency Operations Center and each regional office has secure facsimile capability. The NRC Telephone Directory provides information on the locations and telephone numbers of secure facsimiles at NRC. (i)

Submit requirements for secure telecommunications equipment to the Director, DFS. Requests must clearly identify requirements and be appropriately justified. Ensure that no classified or sensitive unclassified data is included in the request. DFS will evaluate and verify each request and initiate the necessary procurement actions. (ii)

Automatic Digital Network (AUTODIN) (b)

The NRC DFS operates an AUTODIN system in the Secure COMCtr, Room O-2D6. The AUTODIN receives and transmits classified and unclassified messages within the Federal Government to include the Department of Defense; civil agencies (e.g., Federal Bureau of Investigations, Federal Emergency Management Agency, Department of Energy); embassies; and some non-governmental agencies such as the International Atomic Energy Agency (IAEA). Information received includes diverse national or international information or activities involving or relating to nuclear power or nuclear materials safety and safeguards, terrorist activities worldwide, threats and hostile actions against nuclear facilities, nuclear incidents worldwide, travel advisories, and IAEA international cooperation. (i)

Secure Telecommunications Systems at NRC (F) (continued)

Record Telecommunications (4) (continued)

AUTODIN is capable of sending and receiving classified and unclassified message traffic at various levels of classification and precedence categories. The Secure COMCtr operates daily during normal working hours, and DFS has procedures for emergencies. Contact the Information Security Branch for additional information on accessing this network. (ii)

Microcomputers (PCs) (c)

Any telecommunication of classified information, Safeguards Information (SGI), or sensitive unclassified information, using an AIS, whether network or standalone, must meet the requirements of MD 12.5.

Voice Telecommunications (5)

General (a)

Classified or sensitive unclassified voice telecommunications, whether by telephone, radio, video-teleconferencing, or another means, should be transmitted over protected systems to the maximum degree possible. The STU-III is the NRC-preferred telephone for voice transmission of classified and sensitive unclassified information. Submit requests for STU-III telephones in writing to the Director, DFS. Resident inspectors requesting secure voice capability should submit the request through the regional COMSEC custodian for concurrence. Requests for other secure telecommunications equipment should be submitted to the Director, DFS. (i)

Requests should include a point of contact, intended location of the STU-III telephone, anticipated number of users, and justification of the need for secure voice capability. Requests must clearly identify requirements and be appropriately justified. Ensure that no classified or sensitive unclassified data is included on the request. DFS will evaluate and verify each request and initiate the necessary procurement actions. (ii)

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

Secure Telephone Unit-Third Generation (STU-III), Type 1 Terminal (b)

The STU-III is a self-contained secure analog telephone unit and data transmitter that fits on top of a desk. It uses public-switched telephone network circuits to establish an ordinary dial-up telephone communication path, then, by inserting a terminal-unique crypto-ignition key (CIK) into the telephone, and pushing the "Secure" button, can encrypt voice and data communications worldwide. There are over 300,000 STU-III telephones in use throughout the U.S. Government. The Type 1 terminal has been endorsed by the NSA for securing classified or sensitive unclassified information, when appropriately keyed.

NRC Doctrine for the STU-III, Type 1, Telephone (i)

- The STU-III may be located in areas ranging from a true-type vault to a private office. The location must provide audio privacy to protect information being discussed. (*a*)
- The STU-III must be inventoried daily or upon opening of the room where the telephone is located. The survey should consider signs of tampering and physical or cryptographic insecurities. Loss or possible compromise of the STU-III must be reported to the COMSEC custodian immediately, who then must report it to NRC COR. COMSEC custodians must conduct a physical sight inventory of all STU-III equipment annually, and should sight the equipment twice a year as part of the semiannual COMSEC inventory. (*b*)
- The STU-III is a CCI and must be protected in accordance with NSTISSI No. 4001, "Controlled Cryptographic Items." NRC requires that it also be protected as a high value item. (*c*)
- INFOSEC, will, upon installation of an STU-III, provide any necessary training to the holders and users on the proper operation and protection of the STU-III. Regional COMSEC custodians will provide training to their holders and users. It is the holder's responsibility to ensure that only those appropriately cleared individuals have access to the CIK. (*d*)

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

- COMSEC custodians should periodically inspect STU-IIIs installed in locations accessed by unescorted cleaning crews or non-cleared personnel, for evidence of tampering. Any evidence of tampering must be reported to the Director, DFS, as a COMSEC incident, and the STU-III telephone must be removed from operation pending a determination by the proper authorities of the actions to be taken. (*e*)
- When stored in the same room as the STU-III, CIKs must be placed in GSA-approved security containers. CIKs stored in areas apart from STU-III may be kept in a locked cabinet or desk drawer. Master CIKs are not provided to STU-III holders or users and will remain in the COMSEC custodian's custody at all times. (*f*)
- STU-III users should not normally keep CIKs in their personal possession (e.g., on a key ring or in a purse) or outside the building in which the corresponding STU-III is located. This course of action minimizes possible loss of CIKs and maximizes the availability of CIKs for authorized use. (*g*)
- CIKs must be placed in locked GSA-approved security containers in those areas in which cleaning crews have unescorted access. CIKs must never be left in an unattended STU-III, regardless of its location, and users must ensure that the CIK is secured after their calls are completed. (*h*)
- At the end of each business day, the office to which the STU-III is assigned must ensure that no CIK is left in the STU-III overnight and that all CIKs are properly stored. (*i*)
- Any relocation of a STU-III terminal, whether temporary or permanent, must be reported to the COMSEC custodian, who then notifies the guard force of the relocation. If a STU-III is no longer required, contact the COMSEC custodian for disposition instructions. (*j*)

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

- The STU-III telephone must be electronically rekeyed annually or when directed. At the present time, the annual electronic rekeying is performed by the COMSEC custodians. NSA recommends that the STU-III telephones be rekeyed more often, if possible. STU-III holders can perform electronic rekeying by inserting the CIK and turning it 1/4 clockwise; placing a call to EKMS (1-800-635-6301); and waiting until new operational key is downloaded. If any problems occur during rekeying, contact your COMSEC custodian for assistance. (*k*)
- All COMSEC incidents related to the loss, compromise, or possible compromise of STU-III equipment or keys must be reported immediately by secure means to the NRC COR, which immediately reports to the Director, DFS. The Director, DFS, will determine any additional reporting requirements and take whatever reporting actions are necessary in accordance with existing NSA COMSEC reporting procedures. (*l*)

User Responsibilities (ii)

STU-III users are responsible for the proper use and control of their terminals and CIKs. Responsibilities include:

- Using the secure mode when discussing classified or sensitive unclassified information (*a*)
- Closing the door to the room when using the telephone in the secure mode so that the conversation will not be overheard by persons without the need-to-know (*b*)
- Adhering to the security classification displayed on the terminal for each call (*c*)
- When the terminal is keyed, limiting access to those with a proper clearance and need-to-know (*d*)
- Ensuring only those appropriately cleared individuals have access to the CIK (*e*)

Secure Telecommunications Systems at NRC (F) (continued)

Voice Telecommunications (5) (continued)

- Ensuring that the CIK is not left unattended in the STU-III terminal, and that the CIK is secured upon completion of the call (*f*)
- Checking the STU-III at the end of the day to ensure that a CIK has not been left in the unit and initialing the NRC Form 700 (*g*)
- Reporting COMSEC incidents to the COMSEC custodian or NRC COR. (*h*)

Key Management (iii)

The policy for the management of Type 1 keying material is contained in EKMS 702.01, "STU-III Key Management Plan," and supplements published by NSA. Questions about NRC key management should be directed to the appropriate COMSEC custodian, the NRC COR, or the STU-III Command Authority. These offices and staff members maintain copies of the plan and supplements.

Hand-Receipts and Inventories (iv)

COMSEC custodians are required to perform semiannual inventories and issue hand-receipts to holders of COMSEC equipment.

STU-III Cellular (c)

The NRC has portable cellular STU-III briefcases that can transform desktop STU-IIIs into mobile units with cellular and land line transmission capability. Contact the appropriate COMSEC custodian or the NRC COR for additional information.

Exhibit

Format and Guidelines

for a

Secure Telecommunications Facility Proposal or Plan

Exhibit

Contents

Exhibit

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

1 Introduction

The format and guidelines cover the proposal requirements for both NRC contractors and NRC organizations.

If the proposed system contains a central processing unit or a personal computer, it is also necessary to refer to Handbook 12.5, "NRC Automated Information Systems Security Program," because such a system will be processing as well as transmitting classified data.

The complete proposal may be classified. It should be given a classification review and handled as classified in its draft form.

A coordination sheet should be attached to the front of the proposal and contain the appropriate coordination signatures (see the attachment to this exhibit).

2 Secure Telecommunications

Telecommunications systems prepare, transmit, communicate, or process information (e.g., writing, images, sounds) by electrical, electromagnetic, electromechanical, electro-optical or electronic means, using media such as telephone lines, cable, microwave, satellite, etc. Telecommunications systems include, but are not limited to, telephones, facsimiles, radios, video and video-teleconferencing, networks (e.g., LANs and WANs), or other data transmission systems.

Classified information may not be telecommunicated unless the telecommunications system has been approved by the Director, Division of Facilities and Security (DFS), Office of Administration. The NRC office requesting approval of a telecommunications facility must submit a security proposal using the format provided below. Submit the proposal to the Director, DFS, for evaluation and approval.

2.1 Justification for the Need for Secure Telecommunications

Justify the need for secure voice and/or data communications. Discuss the classification levels (e.g., secret or confidential); categories of information (e.g., national security information (NSI) or restricted data (RD)); and the types of information (e.g., material control and accountability information) being transmitted.

2.2 Duration and Nature of Activity

Indicate if this is an ongoing requirement or if short-term and the probable duration of the telecommunications activity.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

2.3 Supplementary Glossary of Terms

Define any special terminology applicable to the telecommunications system that may be system-unique or not defined in NSTISSI 4009, "National Information Systems Security (INFOSEC) Glossary."

The terms "Secure Communications Center" and "Telecommunications Facility," refer to a type of facility dedicated to the preparation, transmission, communication or related processing of information. Unless otherwise noted, both terms refer to both attended and unattended facilities.

2.4 Equipment and Media

List all equipment and media that comprises the secure telecommunications system, including terminal equipment, cryptographic equipment, modems, switching systems, signaling equipment, and testing equipment. If the telecommunications system is to be networked, describe the network media used, e.g., twisted pair cable, coaxial cable, fiber optic cable, microwave, satellite, or combinations of media (e.g., a network system that uses Ethernet cabling throughout a building, but fiber optic cabling between buildings).

Provide the manufacturer's name and the model number of each piece of equipment.

2.5 System Functional Block Diagram

By means of a complete system functional block diagram, show the functional interrelationship of all equipment associated with the secure telecommunications system, including terminal equipment, cryptographic equipment, and modems. If the telecommunications system is to be networked, provide the network security architecture, specifically addressing security-relevant issues. All interconnected nodes on the network should be provided on the block diagram. Provide a brief narrative description, as necessary, to supplement the diagram.

2.6 Communications Security (COMSEC)

COMSEC is a program in which the National Security Agency (NSA) acts as the central procurement agency for the development and, in some cases, the production of INFOSEC items. The NSA certifies cryptographic and other communications security products such as key, equipment, devices, documents, firmware, or software that

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

embodies or describes cryptographic logic or performs COMSEC functions. COMSEC is considered especially sensitive because of the need to safeguard U.S. cryptographic principles, methods, and material against exploitation.

2.6.1 COMSEC Accounts

COMSEC accounts are administrative entities, identified by an account number, used to maintain accountability, custody, and control of COMSEC material.

Discuss the COMSEC account(s) that exists or is planned. Provide the name, address, and telephone number of the Central Office of Record (COR) of the COMSEC account (if already established). Discuss the contents of the COMSEC account inventory in general terms only (e.g., the holdings in this account include the secure telephone units [STU-IIIs], Type 1 seed key, traditional key, electronic key, KG-84s, and the data encryption standard key). If additional information is required, the NRC will contact the COR of the account.

NOTE: Not all equipment and material associated with a telecommunications system is COMSEC accountable and this equipment may be different than the equipment listed in Section 2.4.

2.6.2 COMSEC Custodians and Alternates

Designate the names, titles, and qualifications (citizenship, possess a valid "Q" clearance, COMSEC or related experience, training) of the individuals who have been selected as the COMSEC custodian and alternate(s).

Because of the sensitivity of COMSEC material and the rigid controls required, the COMSEC custodian and alternate(s) must possess exemplary qualities. Ensure that the individuals selected:

- Are responsible individuals qualified to assume the duties and responsibilities of a COMSEC Custodian
- Are in a position or level of authority that will permit them to exercise proper jurisdiction in fulfilling their responsibilities
- Have not been previously relieved of COMSEC custodian duties for reasons of negligence or nonperformance of duties

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

- Are in a position that will permit maximum tenure (not less than 1 year)
- Will not be assigned duties that will interfere with their duties as COMSEC custodian or alternate
- Are actually performing the custodial functions on a day-to-day basis (The COMSEC custodian position will not be assumed solely for the purpose of maintaining administrative or management control of the account functions.)
- Hold grade GG-7 or above

2.6.3 COMSEC Material Accountability

Describe how the accountability of COMSEC materials and documents is maintained (e.g., under NRC oversight, the Department of Energy (DOE) oversight, or NSA oversight).

2.6.4 Storage, Transportation, Reproduction, and Destruction of COMSEC Material

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4005, "Safeguarding COMSEC Facilities and Material," establishes the minimum national standards for safeguarding COMSEC material.

Describe how COMSEC material is/or will be stored, transported, reproduced, protected, and destroyed. In the case of destruction of accountable COMSEC documents and keying material, state the type, manufacturer, and model number of any destruction equipment (e.g., shredders) you would like to have considered by the Director, DFS, as approved equipment. Describe the techniques used in the destruction process (e.g., mixture of classified material with unclassified material, and the method of disposal of the waste material).

2.6.5 COMSEC Training

Discuss COMSEC training (e.g., ND-112, NSA COMSEC Custodian Course) previously received (include dates) by COMSEC custodian or alternates (e.g., DOE COMSEC training or NSA COMSEC training). Indicate the number of people requiring training, the approximate timing for such training, and the name and title of the individual who will coordinate the training.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3 Fixed COMSEC Facilities, Telecommunications Facilities, Secure Communications Centers

NSTISSI 4005 establishes the minimum national standards for constructing and protecting COMSEC facilities, wherein the primary purpose is generating, storing, repairing, or using COMSEC material.

Work areas not considered COMSEC facilities that contain COMSEC equipment (e.g., STU-IIIs, KG-84s, and/or data transfer devices) must be protected in a manner that affords protection at least equal to what is normally provided to other high value and sensitive material and ensure that access and accounting integrity is maintained.

3.1 Physical Security

Describe the physical location of the facility within its host building. Discuss the functions and relative locations of adjacent buildings and rooms. Describe the construction of the facility, to include walls, floors, ceilings, main entrance door, other doors, door locks, windows, other openings, and security systems in place (e.g., intrusion alarms, armed guards, and/or video cameras).

Describe the procedures for daily security checks (e.g., visual checks are made at least once every 24 hours on a random basis by personnel assigned to the facility).

Provide initial and latest reinspection reports, technical security evaluation (TSE) report, and TEMPEST countermeasures and verification reports, if applicable.

3.2 Access Lists

Discuss requirements for access to the secure facility. Include the functional titles of the individuals who will routinely access the facility. Provide the title of the official who will generate the access lists and the method to be used for keeping the list up to date.

3.3 Visitor Control

A visitor register must be maintained at the facility entrance area to record the arrival and departure of authorized visitors. Describe the format of the log, requirements for the monitoring of visitors while in the facility, how personnel security clearances are verified, and what personal identification is required for access to the facility.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.4 Intrusion Alarm System/Protective Personnel

Describe the type of intrusion alarm system (e.g., infrared, ultrasonic) used to protect the facility and where the alarm annunciates. Specify the required response time of protective personnel, if the alarm is activated.

3.5 Protecting Passwords and Lock Combinations

Describe the method used for protecting combinations for the secure facility. Refer to NSTISSI 4005 for the requirements for controlling the combinations of containers used to store COMSEC documents and material. Describe the written instructions furnished to the secure facility's personnel and users for controlling combinations.

3.6 Destruction

Identify the pertinent types of classified media (e.g., printed or magnetic storage media) involved in the activities of the secure facility and the classification of the media (e.g., Secret-National Security Information, Secret-Restricted Data).

Describe the methods of both routine and emergency destruction of each type of media (e.g., shredding, degaussing). See NSTISSI 4004, "Routine Destruction and Emergency Protection of COMSEC Material (U)," for guidance in the destruction of COMSEC material.

3.7 Floor Plans and Drawings

Provide the following:

Floor plans of the secure facility showing the location of all equipment, including all terminals, related cryptographic equipment, modems, and other telecommunications equipment

- Floor plans showing the construction of walls, floor, and ceiling of the room(s) containing the secure equipment
- Separate architectural details such as doors, windows, and ducts
- Floor plans that indicate the type of facilities and operations in the areas adjacent to and on the floors immediately above and below the secure facility and installation drawings, including wiring diagrams and conduit plans for the secure telecommunications equipment

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.8 TEMPEST

"TEMPEST" is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when transmitted, received, handled, or otherwise processed by any information processing equipment.

TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security, should the information be obtained by a foreign intelligence organization.

Identify what TEMPEST countermeasures may be required for the secure facility. If TEMPEST countermeasures are in use at the facility, describe your implementation of the program (e.g., certification, accreditation, zoning, shielding).

3.9 Nonessential Audio/Visual Equipment

Certain U.S. Government-owned or -leased (or company-owned or -leased) items are prohibited in secure facilities unless approved by the Director, DFS, for conduct of official duties. These include two-way transmitting equipment, recording equipment (audio, video, optical), and test, measurement, and diagnostic equipment. Also, certain personally owned electronic equipment items, such as photographic, video, and audio recording equipment; and computers and associated media, are prohibited in secure facilities.

Describe in the plan any telephone, intercom, paging, or music systems that are internal to, or penetrate the secure facility. Verify and certify that there are no fortuitous conductors, speakers that can be reversed to be used as microphones, or telephones that can be rewired to be used as microphones. Pay particular attention to any wire penetrations into the secure facility by any system operated or controlled from outside the facility. This section of the plan also should describe the controls and restrictions imposed on personnel bringing electronic devices into the secure facility.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.10 Technical Security Evaluation (TSE)

All reasonable countermeasures should be taken to ensure that there are no clandestine surveillance devices in secure telecommunications facilities. Evaluations for clandestine surveillance devices should be conducted as appropriate to the threat level determined by the Director, DFS. These evaluations should be considered when facilities are initially activated or reactivated after foreign occupation, or when there is known or suspected access by foreign maintenance or construction personnel, or when clandestine surveillance or recording devices are suspected in or near a secure facility. Any actual or suspected clandestine surveillance or recording devices must be reported in accordance with the requirements of NSTISSI 4003, "Reporting and Evaluating COMSEC Incidents."

Describe any tests or inspections of the secure facility that are planned or have already been performed. Indicate the frequency of the testing, the reason for the frequency (e.g., type, purpose, and classification level of the information handled at the secure facility, or specific equipment contained therein), and if the tests and inspections include external sound attenuation tests and audio countermeasure tests to detect clandestine "eavesdropping" devices.

Provide a list of tests to be performed, copies of the specific test procedures to be used, and the name of the contractor(s) performing the tests to the Director, DFS, for approval. If the tests have already been conducted, provide a copy of the test results to the Director, DFS, for approval.

3.11 COMSEC Inspections

A COMSEC inspection should be conducted prior to initial activation where practical, but must be conducted within 90 days after activation. Thereafter, facilities must be reinspected based on threat, physical modifications, sensitivity of programs, and past security performance. At a minimum, the inspection must address secure operating procedures and practices, handling and storage of COMSEC material, and routine and emergency destruction capabilities.

Describe the procedures, either in place or planned, for conducting COMSEC inspections.

Exhibit (continued)

Format and Guidelines for a Secure Telecommunications Facility Proposal or Plan

(continued)

3.12 Unattended Secure Telecommunications Facilities

Unattended secure telecommunications facilities must be protected by an intrusion detection system or guarded in accordance with NSTISSI 4005.

Describe any special security controls in place for unattended secure telecommunications facilities. Information on response time to an alarm, storage of keyed COMSEC equipment and maintenance manuals, procedures for inspection of the facility, and emergency procedures, should be addressed in the plan.

Attachment

Coordination Sheet

Director of Facilities and Security
Office of Administration

Director, Division of Contracts and
Property Management, ADM

Director, Division of _____ or Regional Administrator _____

Prepared by