

ORDER

**DRAFT
DOE O 205.2**

Approved: XX-XX-XX

DEPARTMENT OF ENERGY TELECOMMUNICATIONS SECURITY PROGRAM



**U.S. DEPARTMENT OF ENERGY
OFFICE OF THE CHIEF INFORMATION OFFICER**

DEPARTMENT OF ENERGY TELECOMMUNICATIONS SECURITY PROGRAM

1. **PURPOSE.** To set forth requirements and responsibilities for the U.S. Department of Energy (DOE) Telecommunications Security Program (TSP) in accordance with National policy specifying measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications.

The Telecommunications Security Program objectives:

- a. supplement DOE Order 205.1B Cyber Security Program;
 - b. implement National policies from the Committee on National Security Systems (CNSS) for the following Telecommunications Security Programs:
 1. Communications Security (COMSEC) that includes Cryptographic/COMSEC Access;
 2. Emissions Security (TEMPEST); and
 3. Protected Distribution Systems (PDS) that includes Classified Distributive Information Networks (CDIN) and Protected Transmission Systems (PTS);
 - c. provide telecommunications facilities and services which fulfill COMSEC requirements under normal and emergency conditions;
 - d. establish a training and education program that develops and maintains telecommunications security competencies throughout the DOE Federal and contractor workforce and enables personnel to fulfill their responsibilities in supporting the Telecommunications Security Program;
 - e. ensure the secure installation of classified information processing equipment, installation and operation of crypto-equipment, secure transmission of classified information and sensitive unclassified COMSEC information, and protection of cryptographic principles and methods; and
 - f. operate a central office of record and a communications security material control system to direct, manage, and control the acquisition, distribution, accountability, and disposition of communications security materials within the Department.
2. **CANCELLATION.** *DOE M 205.1-3, Telecommunications Security Manual*, dated 4-17-2006.

Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect

throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

a. Departmental Applicability. This directive applies to all Departmental elements that process or transmits classified information.

- (1) The Administrator of the National Nuclear Security Administration (NNSA) must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.
- (2) In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.
- (3) The Administrator of Bonneville Power Administration (BPA) will assure that BPA employees and contractors comply with their respective responsibilities under this directive.
- (4) For the purposes of this Order, the following Departmental elements are identified as Senior DOE Management (SDM) and are responsible for implementing the DOE Telecommunications Security Program requirements described in this Order:
 - (a) The Office of the Under Secretary of Energy
 - (b) The Office for the Under Secretary of Science
 - (c) The National Nuclear Security Administration
 - (d) The Office of the Chief Information Officer (OCIO)

b. DOE Contractors. Except for the equivalencies/exemptions in Paragraph 3.c., the CRD sets forth requirements of this Order that will apply to contracts that include the CRD.

- (1) The CRD Attachment 1, sets forth requirements of this directive that will apply to Contractors that process, transmit, or receive classified information on behalf of DOE, including NNSA.
 - (2) As stated in DEAR clause 970.5204-2, titled *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and incur only costs that would be incurred by a prudent person in the conduct of competitive business.
 - (3) Heads of Field Elements and Headquarters Departmental Elements. Ensure that the requirements of the CRD of this directive or other appropriate telecommunications security requirements are included in the contract.
 - (4) Contracting Officers. Once notified, contracting officers are responsible for incorporating this directive into the affected contracts via the Laws, Regulations, and DOE Directives clause of the contracts.
- c. Equivalencies/Exemptions for DOE O 205.2. Requests for equivalencies and exemptions from Paragraph 4, *Requirements* of this Order must follow the Deviation Approval Process defined in *Attachment 3*.
- (1) Equivalencies. Conditions that technically vary from the DOE telecommunications security criteria in this Order, but affords equivalent levels of protection. The TEMPEST Program and the PDS Program permit equivalencies and must be approved through the Deviation Approval Process detailed in *Attachment 3*.
 - (2) Exemptions. Deviations from the criteria in this Order that create vulnerability because corrections to the nonstandard conditions are not feasible or are inadequate. The COMSEC, TEMPEST, and PDS Programs permit exemptions and must be approved through the Deviation Approval Process detailed in *Attachment 3*.

4. REQUIREMENTS.

a. This section applies to DOE Telecommunications Security Programs.

- (1) National policies, directives, instructions and other guidance are available through unclassified and classified (SIPRNET) NSA websites. DOE Central Office of Record (COR) / DOE Certified TEMPEST Technical Authority (CTTA) Office will provide copies or access to unavailable national policies.
- (2) The DOE COR/CTTA Office is the final authority on all COMSEC, TEMPEST and Protected Distribution Systems matters.
- (3) Training:
 - (a) Security training and briefings are developed, maintained and administered to DOE employees commensurate with their involvement with the Telecommunications Security Program.
 - (b) Training of DOE Telecommunications Security Program appointed personnel for all Headquarters and field organizations is conducted by or arranged for by the DOE COR/CTTA Office. Appointed personnel may be trained temporarily by experienced appointed personnel at a field organization if the DOE COR/CTTA Office training is not readily available. The formal DOE COR training must be attended within 6 months of the appointment date. The CTTA provided training must be attended within a year of the appointment date.
- (4) Telecommunication Security Program Incident Reporting Requirements.
 - (a) COMSEC. All COMSEC incidents are reported to the DOE COR according to *National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4003, Reporting and Evaluating COMSEC Incidents.*
 - (b) TEMPEST. All TEMPEST incidents are reported to the DOE CTTA according to *CNSS Policy (CNSSP) No. 300, National Policy on Control of Compromising Emanations.*
 - (c) Protective Distribution Systems (PDS). All PDS incidents are reported to the DOE CTTA according to *NSTISSI No. 7003, Protective Distribution Systems (PDS).*

b. Communications Security (COMSEC) Program. This section provides information and requirements for the operation and maintenance of DOE secure

communications activities for the acquisition, storage, assignment, distribution, inventory, control, and accountability of COMSEC material applicable to COMSEC activities of DOE.

- (1) Access, storage, handling, distribution and classification marking must be implemented according to *NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials* and DOE requirements defined in this Order.
- (2) Accounting for COMSEC Material. Controlled Cryptographic Items (CCI) equipment and components will be accounted for and controlled through the DOE COMSEC Material Control System (CMCS) according to *NSTISSI No. 4001, Controlled Cryptographic Items*.
- (3) Nomenclature. The nomenclature for COMSEC material is commonly known as the short title. The nomenclature system for identification of National Security Agency (NSA)-produced or authorized United States (U.S.) COMSEC material must be executed according to *National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) COMSEC/1-93, Nomenclature for Communications Security Material*.
- (4) Contacting NSA. In collaboration with NSA, it has been established that all requests, inquiries, and requirements for the DOE Telecommunications Security Program that would involve NSA must be processed through the DOE COR /CTTA Office. Those accounts that have established User Representative Accounts for ordering modern keying material may continue to directly process those requests and interface with the Central Facility (CF) as required. This is the only office at NSA that personnel are authorized to contact directly, unless otherwise specified by written approval by the DOE COR/ TTA Office.
- (5) Inventory Requirements for COMSEC Material. The CMCS for DOE is classified Confidential. Individual account inventory reports are Official Use Only (OUO), except for those accounts holding Defense Threat Reduction Agency (DTRA) keys that are classified Confidential. Listings of electronic keying material distributed by and accountable to the Electronic Key Management System (EKMS) CF are marked and handled as OUO.
- (6) COMSEC Security Account Operations. General requirements and standard procedures for the operation of DOE and DOE contractor accounts are set forth in *NSTISSI No. 4005* and this

Order. These requirements and procedures apply to all COMSEC accounts processing classified information through a crypto-device, whether it is a communications center environment, a crypto-account operated in an office, or a secure phones only account.

- (7) An equivalency request must be prepared and submitted to the DOE COR Manager through the Deviation Approval Process detailed in *Attachment 3*.
- (8) COMSEC filing requirements. The COMSEC filing requirements, guidelines and procedures are described in *NSTISSI No. 4005*.
- (9) Crypto-Facilities Planning. The requirements, guidelines and procedures in the planning of crypto-facilities are described in *NSTISSI No. 4005*.
- (10) Engineering and Installation of Crypto-Facilities. Crypto-center design, engineering, and installation must be carried out as directed by *NSTISSI No. 4005*.
- (11) Acquisition of COMSEC Material. All accountable COMSEC material, with the exception of modern electronic keying material, must be controlled through the DOE CMCS that is maintained by the DOE COR. All modern electronic keying material must be controlled through the NSA EKMS. The *NSTISSI No. 4005* guidelines, limitations, and procedures for acquisition of COMSEC material and certain crypto-related equipment and supplies are applicable to all DOE organizations except where other arrangements are specifically authorized by the DOE COR.
- (12) Distribution of COMSEC Material. Crypto-marked material and accountable crypto-related material must be distributed through the Department COMSEC distribution channel in accordance with procedures described in *NSTISSI No. 4005*.
- (13) Cryptographic High Value Products (CHVP) must be carried out as directed by *CNSSI No. 4031*.
- (14) Other COMSEC Account Operations.
 - (a) Interdepartmental Crypto-operations. Requirements, acquisition of network facilities, accountability of COMSEC material, and operating procedures applicable to interdepartmental crypto-operations must be coordinated with the DOE COR Manager.

- (b) Crypto-operations Outside Continental United States. Operation of DOE crypto-systems outside the Continental United States (CONUS) is subject to prior approval by the DOE COR Manager and coordination with the NSA. Information regarding proposed crypto-operations outside CONUS must be submitted to the DOE COR Manager.
 - (c) Non-cryptographic Secure Communications. The transmission of classified information without encryption is subject to the Telecommunications Security Program requirements cited in this Order.
 - (d) Encryption of Sensitive Unclassified Information in Support of COMSEC Operations. Unclassified crypto-equipment used to protect sensitive unclassified COMSEC information is available from commercial vendors. These products must comply with *National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules*. Products must be validated to *FIPS PUB 140-2* and other cryptography based standards through the Cryptographic Module Validation Program (CMVP).
- (15) Maintenance of COMSEC Equipment.
- (a) Periodic maintenance and repair of COMSEC equipment used by DOE is furnished by DOE COMSEC appointed personnel who have been certified by completing NSA approved vendor training.
 - (b) Vendors authorized by the NSA will also perform maintenance as required on crypto-equipment. NSA will specify which equipment must be returned to the vendor depot for maintenance or upgrades.
- (16) COMSEC Audits and Surveys.
- (a) Representatives from the DOE COR Manager's office will conduct the audit to ensure COMSEC accounts are complying with applicable requirements governing accountability, handling, and safeguarding of COMSEC material, as required in *NSTISSI 4005*. These audits will be conducted on a biennial basis, or more often, if required. Notification of the audit and crypto-facility survey will be sent to the responsible Federal office at least 30 days prior to the scheduled visit. The COMSEC Custodian and, if possible, the cognizant Control Officer must accompany the personnel conducting the audit.

- (b) Copies of the COMSEC audit and survey report with a statement of required corrective actions, if any, will be furnished to the responsible program, field, or site office, as applicable.
 - (c) The continued use of COMSEC equipment and materials is subject to a biennial review as part of the COMSEC Audit and Crypto-facility COMSEC Survey Program. The DOE COR Manager will advise the account personnel of actions required should there be a change in account operations that result in a reduction of account holdings and activities.
- (17) Emergency Protection of Materials. The *NSTISSI No. 4004.1, Routine Destruction and Emergency Protection of COMSEC Material* provides requirements, guidance and information regarding the protection of COMSEC material under emergency conditions. The approval authority for DOE created documentation for routine destruction and emergency protection of COMSEC material is the DOE COR Manager.
 - (18) Routine and Emergency Destruction Plans. The requirements, guidelines and procedures to be followed for Routine and Emergency Destruction Plans are described in *NSTISSI No. 4004.1*. A sample of each plan is included in the *DOE Communications Security (COMSEC) Program Supplemental (DRAFT) Guide*.
 - (19) For additional guidance regarding formal cryptographic access and COMSEC Access Programs, refer to the *DOE Communications Security (COMSEC) Program Supplemental (DRAFT) Guide*.
 - (20) For additional guidance, processes, and information regarding protecting, storing, handling, and controlling COMSEC material, refer to the *DOE Communications Security (COMSEC) Program Supplemental Guide (DRAFT)* and the *DOE Protected Transmission System (PTS) Program Supplemental (DRAFT) Guide*.
- c. Cryptographic/COMSEC Access Program. DOE and DOE contractor Cryptographic/COMSEC Access Programs must implement *CNSSP No. 3, National Policy on Granting Access to U.S. Classified Cryptographic Information*.

The COMSEC Control Officer will be responsible for implementing the Cryptographic/COMSEC Access Program for their respective account.

- d. Emissions Security (TEMPEST) Program. TEMPEST is a short name referring to investigations and studies of compromising emanations from IT systems which, if intercepted and analyzed, might disclose national security information. The DOE TEMPEST Program determines the need for TEMPEST countermeasures through on-site inspections of information technology (IT) systems for compliance. The DOE CTTA is the Program Manager for the DOE TEMPEST Program.
- (1) General Requirements.
- (a) Each facility or remote operational element is required to determine its threat and TEMPEST vulnerability in accordance with National policy as stated in this Order and *Attachment 5, Classified Technical Section* of this Order. The results of this assessment will determine the emissions countermeasures to be applied.
- (b) The DOE TEMPEST Program implements National policy in accordance with:
- 1 *NSTISSAM 2-95, RED/BLACK Installation Guidelines;*
- 2 *CNSS Policy (CNSSP) No. 300, National Policy on Control of Compromising Emanations; and*
- 3 *NSTISSI No. 7000, TEMPEST Countermeasures for Facilities.*
- (c) Facilities warranting TEMPEST countermeasures are to be designed and built to adhere to the criteria defined in this Order and *NSTISSAM 2-95*.
- (d) Any cost involved with the implementation of TEMPEST countermeasures must be approved by the DOE CTTA before funds can be expended.
- (2) Facility Review and Determination. Facility review and determination must comply with *NSTISSI No. 7000*.
- (a) Threat Environment. Refer to the *Attachment 5, Classified Technical Section* of this Order for requirements for Threat Environment Levels.
- (b) IT Systems Separation. All classified IT systems will maintain separation from unclassified systems, lines, and operations in accordance with *NSTISSAM 2-95*.

- (c) Transmission Security criteria are defined in the *DOE Emissions (TEMPEST) Program Supplemental Guide (DRAFT)* and *CNSSP No. 17, Policy on Wireless Communications*.
 - (d) Vulnerable Location. A vulnerable location is subject to TEMPEST countermeasures as defined in NSTISSI No. 7000.
- (3) Determining TEMPEST Countermeasures.
- (a) TEMPEST countermeasures are utilized only after a TEMPEST threat assessment has been conducted and vulnerabilities have been identified. The CTTA retains exclusive authority for approving the implementation of all TEMPEST countermeasures.
 - (b) TEMPEST countermeasures must comply with *NSTISSI No. 7000, NSTISSAM TEMPEST/2-95, NSTISSI No. 7001, NonStop Countermeasures, and CNSSP No. 300*.
 - (c) Outside the United States Criteria. Refer to the *Attachment 5, Classified Technical Section* of this Order.
 - (d) Accountability of Wires/Cables. For a facility under the TEMPEST Program, the accountability of wires/cables must be accomplished according to *NSTISSAM 2-95*.
- (4) TEMPEST RED/BLACK CRITERIA
- (a) Due to security, classification, and Operations Security (OPSEC) requirements, all Special Access Program (SAP) areas will be protected, reviewed, and acknowledged as Top Secret (TS).
 - (b) RF Transmitters. All transmitting devices and associated components (cables, hubs, etc.) that are located within 100 feet of a classified facility will require a Special Review as required in *Attachment 5, Classified Technical Section* of this Order.
 - (c) NSA-approved Keyboard, Video and Mouse (KVM) switches must be used when classified and unclassified central processing units are using the same keyboard, monitor (video) and mouse.
- (5) Basic grounding concepts must follow *MIL HDBK 419 Revision A, Grounding Bonding & Shielding For Electronic Equipment and NSTISSAM 2-95*.
- (6) New Facility Design. Perform new facility design according to *National Agency Communications Security Information Memorandum (NACSIM) No. 5000, TEMPEST Fundamentals* and *MIL HDBK 419*.

- (7) Shielded enclosure designs must be implemented according to *NSTISSAM 1-95* and *MIL HDBK 419*.
- (8) Electromagnetic Interference must be implemented according to *MIL HDBK 419*.
- (9) Fiber Optic installation guidelines must comply with *NSTISSAM 2-95*.
- (10) Sensitive Compartmented Information (SCI). The DOE CTTA and the DOE Senior Intelligence Officer (SIO) have agreed and made it clear to all applicable personnel that the following will apply for all Sensitive Compartmented Information Facilities (SCIF):
 - (a) All SCIF Coordinators must allow their site TEMPEST and PTS Coordinators to conduct a PDS and TEMPEST threat assessment, a special review, and prepare a TEMPEST and PDS plan for each SCIF at their site.
 - (b) National policy protection measures must be implemented according to *NSTISSAM 2-95* and *NSTISSI No. 7003*.
- (11) Requirements for Radio Frequency (RF) Wireless Systems. Procedures must adhere to *CNSSP No. 17, Policy on Wireless Communications: Protecting National Security Information*.
 - (a) Wireless transmitter devices (e.g., Blackberries, cell phones, wireless laptops) are NOT allowed in TEMPEST protected areas unless approved by the DOE CTTA.
 - (b) Laser and Infrared. Must comply with *NSTISSAM 2-95*.
 - 1 Laser and infrared (IR) based systems that are a functional part of any classified accredited system must have the IR emitter/detector concealed with metallic tape, e.g., aluminum foil, copper foil, etc.
 - 2 Must comply with Title 18, Part I, Chapter 37, and Section 798, entitled *Disclosure of Classified Information*.
 - (c) Radio Frequency Identification (RFID) Systems.
 - 1 RFID systems are considered portable electronics and are subject to a Special Review and must meet requirements specified in *DOE M 470.4-2A, Physical Protection*. The DOE CTTA makes all final determinations of countermeasure implementations for RFID.

2 The protection of emanations from transmitters is contained in the National policies: *NSTISSAM 2-95*, *NSTISSI No. 7001*, and *CNSSP No. 17*.

e. Transmission Security Program.

- (1) Refer to the *DOE Emissions (TEMPEST) Program Supplemental Guide (DRAFT)* and *Attachment 2* of this Order for TEMPEST Coordinator responsibilities for Transmission Security.
- (2) Wireless Transmitters Use in Classified Non-TEMPEST Protected Facilities must:
 - (a) be implemented according to *CNSSP No. 17*.
 - (b) include a TEMPEST countermeasure requirements review for the implementation of wireless technologies in facilities under consideration. The review must be completed by the CTTA in accordance with *CNSSP No. 300, National Policy on Control of Compromising Emanations*, and *CNSSI No. 7000, TEMPEST Countermeasures for Facilities*, prior to acquiring wireless National security systems solutions. A TEMPEST countermeasure requirements review is also required for wireless technologies in close proximity to where National security information is discussed or processed.
 - (c) comply with the minimum separation criteria for wireless transmitter devices used in classified facilities protected by the Transmission Security Program that is six (6) feet from all classified equipment and signal/data lines. Additional countermeasures may be required by the CTTA such as greater separation requirements as a result of TEMPEST testing conducted at a specific site for wireless use in a classified area.
- (3) Crypto-Equipment.
 - (a) Crypto-equipment must be treated as both RED and BLACK, and separated from other crypto-equipment based on *NSTISSAM 2-95* separation criteria unless otherwise specifically stated in this Order.
 - (b) Refer to *DOE Emissions (TEMPEST) Program Supplemental Guide (DRAFT)* for separation criteria.
 - (c) Crypto-equipment and its ancillary units must be installed in accordance with applicable NSA criteria.

- f. Protected Distribution Systems (PDS) Program. This program prescribes the technical standards to be applied in the design, installation, and use of PDS for transmitting and receiving classified information that has not been encrypted with NSA Type 1 encryption.
- (1) PDS Requirements.
 - (a) The cognizant site Protected Transmission System Approval Authority (PTSAA) must contact the DOE Telecommunications Security Program Manager (TSPM) for guidance on how to implement PDS requirements.
 - (b) DOE must utilize the following National policy documents in the design, installation, use and maintenance of the PDS program:
 - 1 *NSTISSI No. 7000, TEMPEST Countermeasures for Facilities*, dated 29 November 1993.
 - 2 *NSTISSI No. 7001, NONSTOP Countermeasures*, dated 15 June 1994.
 - 3 *NSTISSAM TEMPEST/2-95, RED/BLACK Installation Guidance*, dated 12 December 1995.
 - 4 *NSTISSI No.7003, Protective Distribution Systems (PDS)*.
 - (c) The utilization of these security countermeasures is based on the site threat assessment and final approval by the PTSAA.
 - (2) PDS Technical and Visual Inspection. Refer to *NSTISSI No. 7003* for National policy. For the technical inspection the PTSAA must determine whether Telecommunications Industry Association (TIA) Tier 1 or Tier 2 Standard 528 testing is appropriate for the technical examination of the classified systems, to include all classified signal/data lines. Tier 1 tests essentially measure length and loss, while Tier 2 testing provides length, loss and trace graph that can be stored and used for analysis at some point in the future. Tests results must be documented in the PDS plan under the section of technical inspection.
 - (3) Inspection/Audit Requirements.
 - (a) PDS Inspection. All PDS are required to have a PDS plan and final approval by the PTSAA or designee before going operational. Final approval of the PDS plan must not be given by the PTSAA or designee until he/she has received documentation of a

satisfactory Technical and Visual inspection. In the event a new PDS will be constructed in such a fashion that when completed it will be concealed making it physically uninspectable, the site PTSAA must approve all construction plans, prior to the start of construction of the PDS for coordination, advice, and assistance as appropriate. The PTSAA will also need to witness the construction stages.

(b) For Transmission of TS through Public Domain:

1 PDS is not approved;

2 NSA Type 1 encryption is required.

(c) Approving Authority. The PTSAA or designee (see *Attachment 2* for PTSAA position description and responsibilities) at the cognizant DOE office that has been approved by the DOE TSPM must approve all PDS plans.

(d) Classification. The PDS plan must be classified in accordance with *DOE O 471.1B, Identification and Protection of Unclassified Controlled Nuclear Information*. The plan must be reviewed by an Authorized Derivative Classifier, as applicable, and protected in accordance with DOE classification guidelines as appropriate.

(4) PDS Plan. The PDS plan must consist of the requirements defined in *NSTISSI No.7003, Protective Distribution Systems (PDS)*.

5. RESPONSIBILITIES.

a. Chief Information Officer (CIO).

- (1) Ensures the Department's Telecommunications Security Program supports and enables the Department's missions and management principles.
- (2) Makes certain that National policy requirements are met for the Department's Telecommunications Security Program.
- (3) Serves as SDM for DOE staff and support offices and Power Marketing Administration (PMAs).
- (4) Requests NSA to appoint the DOE CTTA to fulfill the responsibilities in Paragraph (e). This authority may be further delegated.

- (5) Requests NSA to appoint the DOE COR Manager to fulfill the responsibilities in Paragraph (d). This authority may be further delegated.
- (6) Through the Chief Information Security Officer (CISO) fulfills the responsibilities in Paragraph (b).

b. Chief Information Security Officer (CISO).

- (1) Represents DOE on the Committee on National Security Systems (CNSS).
- (2) On behalf of the CIO, coordinates with the DOE SDM in providing Department-wide direction, administration, and coordination of the DOE Telecommunications Security Program.
- (3) Ensures Telecommunications Security Program personnel are properly appointed if applicable, trained and clearances verified.

c. Senior DOE Management (SDM).

- (1) Coordinates with the DOE CIO in the development and implementation of the DOE Telecommunications Security Program.
- (2) Ensures that each organization and contractor site under their cognizance requiring a Telecommunications Security Program establishes implements and sustains the program in accordance with the requirements of this Order.
- (3) Ensure Telecommunications Security Program personnel are properly appointed if applicable, trained and clearances verified. This authority may be further delegated. Refer to Attachment 2 for further details on responsibilities for appointed positions below:

- (a) Telecommunications Security Oversight Manager (TSOM) A TSOM is a Federal employee, located or assigned to a DOE site that has Federal oversight of a DOE laboratory, field site, or facility. This individual must be appointed in writing to the TSPM. The TSOM must be knowledgeable concerning the requirements of all Telecommunications Security Programs addressed in the Telecommunications Security Order.
- (b) Telecommunications Security Site Manager (TSSM). A TSSM may be either a Federal or contractor employee, and must be assigned to a DOE facility. This individual must be formally

appointed by site management. The TSPM and the applicable TSOM must be notified in writing of all appointments.

- (c) COMSEC Control Officer. This individual is a Federal employee or a contractor who is responsible for overseeing crypto-areas and COMSEC activities.
- (d) Alternate COMSEC Control Officer. This individual is a Federal employee or contractor responsible for assisting the COMSEC Control Officer in the required duties. During periods when the COMSEC Control Officer is unavailable, the Alternate COMSEC Control Officer is authorized and required to perform these duties.
- (e) COMSEC Custodian. This individual is a Federal employee or contractor responsible for safeguarding, controlling, and inventorying all COMSEC material assigned to the specific accounts within an organizational unit or facility
- (f) Alternate COMSEC Custodian. This individual is a Federal employee or contractor responsible for assisting the COMSEC Custodian in the required functions of the Custodian position. During periods when the COMSEC Custodian is unavailable, the Alternate COMSEC Custodian is authorized and required to perform these duties.
- (g) Crypto-operator. This individual is a Federal employee or contractor responsible for using crypto-materials to encrypt, decrypt, or authenticate information.
- (h) TEMPEST Coordinator. The TEMPEST Coordinator position is not identified in National policy. This position was created by DOE and only exists within the DOE TEMPEST Program. A TEMPEST Coordinator, designated in writing to the DOE CTTA Office, must be a DOE Federal employee or contractor who is knowledgeable concerning the requirements of this Order and *Attachment 5, Classified Technical Section* of this Order.
- (i) Alternate TEMPEST Coordinator. The Alternate TEMPEST Coordinator position is not identified in National policy. This position was created by DOE and only exists within the DOE TEMPEST Program. An Alternate TEMPEST Coordinator, designated in writing to the DOE CTTA Office, must be a DOE Federal employee or contractor who assists the TEMPEST Coordinator in required functions of the position.
- (j) Protected Transmission System Approval Authority (PTSAA). The PTSAA is a Federal employee, designated in writing in a

memorandum to the DOE TSPM, who has knowledge concerning the installation, maintenance, and inspection of the PDS program.

- (k) PTS Coordinator. A DOE Federal employee or contractor, appointed by site management and designated in writing to the site PTSAA or designee, who will notify the DOE TSPM in writing of the designation. This individual must have knowledge concerning the installation, maintenance, and inspection of Protected Transmission.
 - (l) Alternate PTS Coordinator. A DOE Federal or contractor employee, appointed by site management and designated in writing to the site PTSAA or designee, who will notify the DOE TSPM in writing of the designation. The Alternate PTS Coordinator will assist the PTS Coordinator in the installation, maintenance, and inspection of Protect Transmission Systems.
 - (m) PTS Inspector. A DOE Federal or contractor employee, appointed by site management and designated in writing to the site PTSAA or designee, who will notify the DOE TSPM in writing of the designation. This individual will provide assistance in conducting technical and/or visual inspections for the site PDS Program.
- d. DOE Central Office of Record (COR) Manager. Approved by NSA and serves as the Headquarters point of contact with DOE field organizations and with other Federal agencies on Department-wide COMSEC and privacy activities. Functions as the DOE COMSEC advisor.
- (1) Reviews requests and proposals. Provides advice, assistance, and direction regarding the design, engineering, installation, operation, and maintenance of COMSEC facilities.
 - (2) Performs as the DOE Command Authority for all EKMS transactions.
 - (3) Serves as the DOE Telecommunications Security Program Manager (TSPM) with responsibility for:
 - (a) developing, implementing and maintaining National policies, standards and procedures governing the COMSEC, Cryptographic/COMSEC Access, TEMPEST, and PDS Programs;
 - (b) approving the appointments of the PTSAA.
 - (4) Serves as the TSOM for DOE staff and support offices and Power Marketing Administration (PMAs).

- e. DOE Certified TEMPEST Technical Authority (CTTA). The DOE CTTA is a Federal employee who has met established certification requirements in accordance with CNSS approved criteria, and is certified and approved by the NSA.
 - (1) Provides detailed requirements, implementation procedures, and guidance for the secure installation of classified equipment and signal/data lines, installation and operation of crypto-equipment, secure transmission of classified information, and protection of cryptographic principles and methods.
 - (2) Provides for all emissions security measures to deny unauthorized persons information of value that might be derived from the intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.
 - (3) Maintains records of all conducted TEMPEST countermeasure reviews and recommendations.
 - (4) Serves as the Departmental single point of contact when interfacing with the NSA about TEMPEST matters.
 - (5) Serves as the PTSAA for DOE staff and support offices and Power Marketing Administration (PMAs).
 - (6) Notifies the Contracting Officers of which contracts must incorporate the CRD.
 - f. Contracting Officers. Once notified of contractor applicability, incorporates the CRD into affected contracts.
6. REFERENCES. See *Attachment 4*.
7. DEFINITIONS. For National policy definitions, refer to *CNSSI No. 4009, National Information Assurance (IA) Glossary*, dated: April 2010. For DOE specific definitions review the *Telecommunications Security Program Supplementary Guides*.
8. CONTACT. Questions concerning this Order must be directed to the Telecommunications Security Program Manager at 301-903-3957.

BY ORDER OF THE SECRETARY OF ENERGY:

Logo
inserted
here after
approval

NAME
Deputy Secretary

CONTRACTOR REQUIREMENTS DOCUMENT (CRD)
DOE O 205.2, Department of Energy (DOE) Telecommunications Security Program

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

Where classified information is processed, transmitted or received, the contractor must comply with the applicable Telecommunication Security Program requirements:

1. General Telecommunication Security Program Requirements

- a. National policies, directives, instructions and other guidance are available through unclassified and classified (SIPRNET) NSA websites. DOE Central Office of Record (COR) / DOE Certified TEMPEST Technical Authority (CTTA) Office will provide copies or access to unavailable national policies.
- b. The DOE COR/CTTA Office is the final authority on all COMSEC, TEMPEST and Protected Distribution Systems (PDS) matters.
- c. Training:
 - (1) establish a training and education program that develops and maintains telecommunications security competencies throughout the DOE contractor workforce and enables personnel to fulfill their responsibilities in supporting DOE's Telecommunications Security Program.
 - (2) Training of appointed personnel for all contractor organizations is conducted by or arranged for by the DOE COR/CTTA Office. Appointed personnel may be trained temporarily by experienced appointed personnel at a field organization if the DOE COR/CTTA Office training is not readily available. The formal DOE COR training must be attended within 6 months of the appointment date. The CTTA provided training must be attended within a year of the appointment date.
- d. Telecommunication Security Program Incident Reporting Requirements. The contractor must establish and maintain an incident management handling and reporting capability that is consistent with the requirements below:
 - (1) COMSEC. All COMSEC incidents are reported to the DOE COR according to *National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4003, Reporting and Evaluating COMSEC Incidents*.

- f. General requirements and standard procedures for the operation of DOE and DOE contractor accounts are set forth in *NSTISSI No. 4005* and this CRD. These requirements and procedures apply to all COMSEC accounts processing classified information through a crypto-device, whether it is a communications center environment, a crypto-account operated in an office, or a secure phones only account.
- g. An equivalency request must be prepared and submitted to the DOE COR Manager through the Deviation Approval Process detailed in *Attachment 3*.
- h. COMSEC filing requirements must be executed according to the requirements, guidelines and procedures described in *NSTISSI No. 4005*.
- i. Crypto-Facilities Planning. The requirements, guidelines and procedures to be followed in the planning of crypto-facilities are described in *NSTISSI No. 4005*.
- j. Engineering and Installation of Crypto-Facilities. Crypto-center design, engineering, and installation must be carried out as directed by *NSTISSI No. 4005*.
- k. All accountable COMSEC material, with the exception of modern electronic keying material, must be controlled through the DOE CMCS that is maintained at the DOE COR. All modern electronic keying material must be controlled through the NSA EKMS. The *NSTISSI No. 4005* guidelines, limitations, and procedures for acquisition of COMSEC material and certain crypto-related equipment and supplies are applicable to all DOE contractors except where other arrangements are specifically authorized by the DOE COR.
- l. Crypto-marked material and accountable crypto-related material must be distributed through the Department COMSEC distribution channel in accordance with procedures described in *NSTISSI No. 4005*.
- m. Cryptographic High Value Products (CHVP) must be carried out as directed by *CNSSI No. 4031*.
- n. Other COMSEC Account Operations.
 - (1) Requirements, acquisition of network facilities, accountability of COMSEC material, and operating procedures applicable to interdepartmental crypto-operations must be coordinated with the DOE COR Manager.
 - (2) Crypto-operations Outside Continental United States. Operation of DOE crypto-systems outside the Continental United States (CONUS) is subject to prior approval by the DOE COR Manager and coordination with the NSA. Information regarding proposed crypto-operations outside CONUS must be submitted to the DOE COR Manager.

- (3) The transmission of classified information without encryption is subject to the Telecommunications Security Program requirements cited in this CRD.
- (4) Encryption of Sensitive Unclassified Information in Support of COMSEC Operations. Unclassified crypto-equipment used to protect sensitive unclassified COMSEC information is available from commercial vendors. These products must comply with *National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules*. Products must be validated to *FIPS PUB 140-2* and other cryptography based standards through the Cryptographic Module Validation Program (CMVP).

o. Maintenance of COMSEC Equipment.

- (1) Periodic maintenance and repair of COMSEC equipment used by DOE contractors is furnished by DOE COMSEC appointed personnel who have been certified by completing NSA approved vendor training.
- (2) Vendors authorized by the NSA will also perform maintenance as required on crypto-equipment. The NSA will specify which equipment must be returned to the vendor depot for maintenance or upgrades.

p. COMSEC Audits and Surveys.

- (1) Representatives from the DOE COR Manager's office will conduct the audit to ensure COMSEC accounts are complying with applicable requirements governing accountability, handling, and safeguarding of COMSEC material, as required in *NSTISSI 4005*. These audits will be conducted on a biennial basis, or more often, if required. Notification of the audit and crypto-facility survey will be sent to the responsible Federal office at least 30 days prior to the scheduled visit. The COMSEC Custodian and, if possible, the cognizant Control Officer must accompany the personnel conducting the audit.
- (2) Copies of the COMSEC audit and survey report with a statement of required corrective actions, if any, will be furnished to the responsible program, field, or site office, as applicable.
- (3) The continued use of COMSEC equipment and materials is subject to a biennial review as part of the COMSEC Audit and Crypto-facility COMSEC Survey Program. The DOE COR

Manager will advise the account personnel of actions required should there be a change in account operations that result in a reduction of account holdings and activities.

- q. Emergency Protection of Materials. The *NSTISSI No. 4004.1, Routine Destruction and Emergency Protection of COMSEC Material*, provide requirements, guidance and information regarding the protection of COMSEC material under emergency conditions. The approval authority for DOE created documentation for routine destruction and emergency protection of COMSEC material is the DOE COR Manager.
 - r. Routine and Emergency Destruction Plans. The requirements, guidelines and procedures to be followed for Routine and Emergency Destruction Plans are described in *NSTISSI No. 4004.1*. A sample of each plan is included in the *DOE Communications Security (COMSEC) Program Supplemental (DRAFT) Guide*.
 - s. For additional guidance regarding formal cryptographic access and COMSEC Access Programs, refer to the *DOE Communications Security (COMSEC) Program Supplemental Guide (DRAFT)* for assistance.
 - t. For additional guidance, processes, and information regarding protecting, storing, handling, and controlling COMSEC material, refer to the *DOE Communications Security (COMSEC) Program Supplemental Guide (DRAFT)* and the *DOE Protected Transmission System (PTS) Program Supplemental (DRAFT) Guide*.
3. Cryptographic/COMSEC Access Program. The contractor must establish and maintain a Cryptographic/COMSEC Access Program that complies with *CNSSP No. 3, National Policy on Granting Access to U.S. Classified Cryptographic Information*.
- The COMSEC Control Officer will be responsible for implementing the Cryptographic/COMSEC Access Program for their respective account.
4. Emissions Security (TEMPEST) Program. The contractor must establish and maintain a TEMPEST Program that complies with the requirements in Paragraph 4. The DOE CTTA is the Program Manager for the DOE TEMPEST Program.
- a. Each facility or remote operational element is required to determine its threat and TEMPEST vulnerability in accordance with National policy as stated in this CRD and *Attachment 5, Classified Technical Section* of this CRD. The results of this assessment will determine the emissions countermeasures to be applied.
 - b. The DOE TEMPEST Program implements National policy in accordance with:
 - (1) *NSTISSAM 2-95, RED/BLACK Installation Guidelines*;
 - (2) *CNSS Policy (CNSSP) No. 300, National Policy on Control of Compromising Emanations*; and

- (3) *NSTISSI No. 7000, TEMPEST Countermeasures for Facilities;*
- c. Facility Review and Determination. Facility review and determination must comply with *NSTISSI No. 7000 and:*
- (1) Threat Environment must comply with the *Attachment 5, Classified Technical Section* of this CRD for requirements for Threat Environment Levels.
 - (2) All classified IT systems will maintain separation from unclassified systems, lines, and operations in accordance with *NSTISSAM 2-95*.
 - (3) Transmission Security criteria are defined in the *DOE Emissions (TEMPEST) Program Supplemental Guide (DRAFT)* and in *CNSSP No. 17, Policy on Wireless Communications*.
 - (4) A vulnerable location is subject to TEMPEST countermeasures as defined in *NSTISSI No. 7000*.
- d. Determining TEMPEST Countermeasures.
- (1) TEMPEST countermeasures are utilized only after a TEMPEST threat assessment has been conducted and vulnerabilities have been identified. The CTTA retains exclusive authority for approving the implementation of all TEMPEST countermeasures.
 - (2) Facilities warranting TEMPEST countermeasures are to be designed and built to adhere to the criteria defined in this CRD and *NSTISSAM 2-95*.
 - (3) TEMPEST countermeasures must comply with *NSTISSI No. 7000, NSTISSAM TEMPEST/2-95, NSTISSI No. 7001, and CNSSP No. 300*.
 - (4) Outside the United States Criteria. Refer to *Attachment 5, Classified Technical Section* of this CRD.
 - (5) Accountability of Wires/Cables. For a facility under the TEMPEST Program, the accountability of wires/cables must be accomplished according to *NSTISSAM 2-95*.
- e. TEMPEST RED/BLACK CRITERIA
- (1) Due to security, classification, and operations security requirements, all Special Access Program (SAP) areas will be protected, reviewed, and acknowledged as Top Secret (TS).

- (2) All RF transmitting devices and associated components (cables, hubs, etc.) that are located within 100 feet of a classified facility will require a Special Review as required in *Attachment 5, Classified Technical Section* of this CRD.
 - (3) NSA-approved keyboard, video and mouse (KVM) switches must be used when classified and unclassified central processing units are using the same keyboard, monitor (video) and mouse.
- f. Basic grounding concepts must follow *MIL HDBK 419 Revision A, Grounding Bonding & Shielding For Electronic Equipment* and *NSTISSAM 2-95*.
- g. New Facility Design. Perform new facility design according to *National Agency Communications Security Information Memorandum (NACSIM) No. 5000, TEMPEST Fundamentals* and *MIL HDBK 419*.
- h. Shielded Enclosure Designs must be implemented according to *NSTISSAM 1-95* and *MIL HDBK 419*.
- i. Electromagnetic Interference must be implemented according to *MIL HDBK 419*.
- j. Fiber Optic installation guidelines must comply with *NSTISSAM 2-95*.
- k. Sensitive Compartmented Information Facilities (SCIF):
 - (1) All SCIF Coordinators must allow their site TEMPEST and PTS Coordinators to conduct a PDS and TEMPEST threat assessment, a special review, and prepare a TEMPEST and PDS plan for each SCIF at their site.
 - (2) SCIF must implement National policy protection measures defined in *NSTISSAM 2-95* and *NSTISSI No. 7003*.
- l. Requirements for Radio Frequency (RF) Wireless Systems must adhere to *CNSSP No. 17, Policy on Wireless Communications: Protecting National Security Information*.
 - (1) Wireless transmitter devices (e.g., Blackberries, cell phones, wireless laptops) are not allowed in TEMPEST protected areas unless approved by the DOE CTTA.
 - (2) Laser and Infrared must comply with *NSTISSAM 2-95*.
 - (a) Laser and infrared (IR) based systems must have the IR emitter/detector concealed with metallic tape, e.g., aluminum foil, copper foil, etc.

- (b) Must comply with Title 18, Part I, Chapter 37, Section 798, entitled *Disclosure of Classified Information*.
 - (3) Radio Frequency Identification (RFID) Systems.
 - (a) RFID systems are subject to a Special Review and must meet requirements as specified in *DOE M 470.4-2A, Physical Protection*. The DOE CTTA makes all final determinations of countermeasure implementations for RFID.
 - (b) The protection of emanations from transmitters is contained in National policies: *NSTISSAM 2-95, NSTISSI No. 7001*, and *CNSSP No. 17*.
- 5. Transmission Security. The contractor must establish and maintain a Transmission Security Program that complies with the requirements in Paragraph 5:
 - a. Refer to the *DOE Emissions (TEMPEST) Program Supplemental Guide (DRAFT)* and *Attachment 2* for TEMPEST Coordinator responsibilities for Transmission Security.
 - b. Wireless Transmitters Use in Classified Non-TEMPEST Protected Facilities must:
 - (1) comply with *CNSSP No. 17*;
 - (2) include a TEMPEST countermeasure requirements review for the implementation of wireless technologies in the facilities under consideration. The review must be completed by the CTTA in accordance with *CNSSP No. 300, National Policy on Control of Compromising Emanations*, and *CNSSI No. 7000, TEMPEST Countermeasures for Facilities*, prior to acquiring wireless National security systems solutions; and on wireless technologies in proximity to where National security information is discussed or processed; and
 - (3) comply with the minimum separation criteria for wireless transmitter devices used in classified facilities protected by the Transmission Security Program that is six (6) feet from all classified equipment and signal/data lines. Additional countermeasures may be required by the CTTA. For any TEMPEST testing conducted at a specific site for wireless use in a classified area, separation criteria will be based on the testing results.
 - c. Crypto-Equipment.
 - (1) Crypto-equipment must be treated as both RED and BLACK, and separated from other crypto-equipment based on *NSTISSAM*

2-95 separation criteria unless otherwise specifically stated in this CRD.

- (2) Refer to *DOE Emissions (TEMPEST) Program Supplemental Guide (DRAFT)* for separation criteria.
 - (3) Crypto-equipment and its ancillary units must be installed in accordance with applicable NSA criteria.
6. Protected Distribution Systems (PDS) Program. Where classified information has not been encrypted with NSA Type 1 encryption, the contractor must establish and maintain a Protected Distribution Systems (PDS) Program that complies with the requirements in Paragraph 6.
- a. The cognizant site Protected Transmission System Approval Authority (PTSAA) must contact the DOE Telecommunications Security Program Manager (TSPM) for guidance on how to implement PDS requirements.
 - b. DOE contractors must utilize the following National policy documents in the design, installation, use and maintenance of the PDS program:
 - (1) *NSTISSI No. 7000, TEMPEST Countermeasures for Facilities*, dated 29 November 1993.
 - (2) *NSTISSI No. 7001, NONSTOP Countermeasures*, dated 15 June 1994.
 - (3) *NSTISSAM TEMPEST/2-95, RED/BLACK Installation Guidance*, dated 12 December 1995.
 - (4) *NSTISSI No.7003, Protective Distribution Systems (PDS)*.
 - (5) The utilization of security countermeasures is based on the site threat assessment and final approval by the PTSAA.
 - c. PDS Technical and Visual Inspection. Refer to *NSTISSI No.7003* for National policy. For the technical inspection the PTSAA must determine whether Telecommunications Industry Association (TIA) Tier 1 or Tier 2 Standard 528 testing is appropriate for the technical examination of the classified systems, to include all classified signal/data lines. Tier 1 tests essentially measure length and loss, while Tier 2 testing provides length, loss and trace graph that can be stored and used for analysis at some point in the future. Tests results must be documented in the PDS plan under the section of technical inspection.
 - d. Inspection/Audit Requirements.
 - (1) PDS Inspection. All PDS are required to have a PDS plan and final approval by the PTSAA or designee before going

operational. Final approval of the PDS plan must not be given by the PTSAA or designee until satisfactory Technical and Visual inspection documentation has been received. In the event a new PDS will be constructed in such a fashion that when completed it will be concealed making it physically un-inspectable, the site PTSAA must approve all construction plans (PTSAA will need to witness the construction stages as well) prior to the start of construction of the PDS for coordination, advice, and assistance as appropriate.

- (2) For Transmission of TS through Public Domain:
 - (a) PDS is not approved for transmission of TS.
 - (b) NSA Type 1 encryption is required.
- e. Approving Authority. The PTSAA or designee (see *Attachment 2* for PTSAA position description and responsibilities) at the cognizant DOE office that has been approved by the DOE TSPM must approve all PDS plans.
- f. Classification. The PDS plan must be classified in accordance with *DOE O 471.1B, Identification and Protection of Unclassified Controlled Nuclear Information*. The plan must be reviewed by an Authorized Derivative Classifier, as applicable, and protected in accordance with DOE classification guidelines as appropriate.
- g. The PDS plan must consist of the requirements defined in *NSTISSI No.7003, Protective Distribution Systems (PDS)*.

TELECOMMUNICATIONS SECURITY PROGRAM APPOINTED POSITIONS AND RESPONSIBILITIES

These positions/responsibilities are in addition to the roles and responsibilities listed in Paragraph 5, Responsibilities, of this Order and CRD.

1. Telecommunications Security Program Site Oversight

- (a) Telecommunications Security Oversight Manager (TSOM). A TSOM is a Federal employee, located or assigned to a DOE site that has Federal oversight of a DOE laboratory, field site, or facility. This individual must be appointed in writing to the TSPM and must be knowledgeable concerning the requirements of all Telecommunications Security Programs addressed in the Telecommunications Security Order. The responsibilities of the TSOM are as follows:
- (1) Must attend the formal DOE-sponsored Telecommunications Security training at least once every four years;
 - (2) Administers and oversees the COMSEC, Cryptographic/COMSEC Access, TEMPEST, and PDS (CDIN/PTS) programs for all DOE laboratories, field sites, and facilities under his/her Federal oversight;
 - (3) COMSEC administrative responsibilities include and are limited to:
 - (a) all documentation related to establishment/closing of COMSEC accounts;
 - (b) appointment memorandums to include all applicable certifications/terminations;
 - (c) Standard Operating Procedures to include annexes/appendices;
 - (d) all documentation regarding correction of audit findings;
 - (e) exemption requests related to COMSEC account; and
 - (f) coordinate with COMSEC Control Officers under his/her cognizance, to receive all COMSEC documents that he/she is administratively responsible for in the COMSEC Program.
 - (4) Serves as the liaison with the DOE TSPM for all telecommunications security activities to include coordination with the site's cyber security organization and appointments of individuals serving in COMSEC roles;
 - (5) Coordinates with the TEMPEST Coordinator when reviewing and assessing the need for transmission security criteria for a classified installation ;

- (6) Can serve as the PTS Approval Authority; and
- (7) Notifies contracting officers which contracts are affected by requirements of the CRD.

(b) Telecommunications Security Site Manager (TSSM). A TSSM may be either a Federal or contractor employee, and must be assigned to a DOE facility. This individual must be formally appointed by site management. The TSPM and the applicable TSOM must be notified in writing of all appointments. In this regard, the applicable TSOM will be responsible for submitting/forwarding this documentation to the TSPM.

- (1) The TSSM must be knowledgeable of the requirements stated in the Telecommunications Security Order related to the program(s) for which he/she is responsible.
- (2) Site management may appoint multiple individuals to function as a TSSM and may designate a specific Telecommunications Security Program responsibility within each appointment.
- (3) Each TSSM must attend all applicable DOE formal training workshops as required in this Order at least once every four years.
- (4) The TSSM will be responsible for local implementation of the COMSEC, Cryptographic/COMSEC Access, TEMPEST, and PDS (CDIN/PTS) Programs, as applicable, for their respective site.
- (5) The TSSM will serve as the liaison to the TSOM for all telecommunications security activities addressed in the DOE Order 205.1B, *Cyber Security Program (draft)* and the *Telecommunications Security Order*.
- (6) The TSSM may also serve in any other position(s) (COMSEC account personnel, PTS Coordinator, TEMPEST Coordinator, etc.) identified within this Order.

2. DOE Communications Security (COMSEC) Program

Additional optional COMSEC roles may be found in NSTISSI No. 3035 or NSTISSI No. 4000.

- a. COMSEC Control Officer. This individual is a Federal employee or a contractor who is responsible for overseeing crypto-areas and COMSEC activities under his/her jurisdiction.

- (1) Provides for and supervises the training of all personnel engaged in crypto-duties;
- (2) Assures that necessary reports are submitted promptly;
- (3) Assures that the proper crypto-system or systems are selected for encryption of each message category;
- (4) Assures that all classified COMSEC material is properly handled;
- (5) Assures that the secure communications facility under his/her jurisdiction is adequately staffed with qualified personnel at all times of operation;
- (6) Administers Cryptographic or COMSEC Access Briefings (to all account personnel requiring access to COMSEC material in performance of official duties. Grants COMSEC access certificates and forwards original access certificates to the DOE COR for retention;
- (7) Prepares (in cooperation with the local security office) a written plan for actions to be taken with respect to the COMSEC material used in the secure communications facility during an emergency. Assures that personnel are trained in their duties under the plan and that appropriate destruction devices are readily available;
- (8) Develops operating procedures as needed to assure secure and efficient COMSEC operations;
- (9) Serves as point of contact for COMSEC maintenance technicians to assure coordination of adequate COMSEC installation and maintenance service including mandatory modifications;
- (10) Serves as point of contact with the DOE COR Manager, other COMSEC Control Officers, and representatives from other COMSEC security offices;
- (11) Ensures that applicable Departmental security directives containing requirements for reporting unofficial foreign travel and contacts with foreign nationals are implemented within the account;
- (12) Ensures that appropriate termination briefings are administered to all personnel who no longer need access to COMSEC material;

- (13) Is authorized to serve as the crypto-technician for the account and perform operator duties; and
 - (14) Attends formal DOE COR COMSEC training once every four (4) years.
- b. Alternate COMSEC Control Officer. This individual is a Federal employee or contractor responsible for assisting the COMSEC Control Officer in the duties listed above. During periods when the COMSEC Control Officer is unavailable, the Alternate COMSEC Control Officer is authorized and required to perform these duties.
- c. COMSEC Custodian. This individual is a Federal employee or contractor responsible for safeguarding, controlling, and inventorying all COMSEC material assigned to the specific accounts within an organizational unit or facility. Specifically this individual:
- (1) Maintains adequate records of COMSEC material sufficient to permit the preparation and submission of COMSEC material reports as required;
 - (2) Maintains records of appointments and changes of COMSEC Control Officer, COMSEC Custodians, COMSEC sub-accounts, Operators, and Alternates having access to COMSEC materials;
 - (3) Performs or verifies proper routine destruction of crypto-material and maintains adequate records of destruction including certification of a witness appointed to the account in each case;
 - (4) Conducts physical inventories of accountable COMSEC material as required;
 - (5) Assists the responsible DOE COR Manager representatives and the COMSEC Control Officer in the conduct of COMSEC audits and COMSEC crypto-facility surveys of accounts and sub-accounts;
 - (6) Notifies the COMSEC Control Officer of all known occurrences that may adversely affect the security of telecommunications and assists in the conduct of related investigations and reports;
 - (7) Assures that COMSEC material is kept posted with current amendments and is readily available to properly authorized individuals;
 - (8) Performs or verifies that required daily inventories (as applicable) are conducted for account keying material and all STE keying material that has not been introduced into a unit;

- (9) Maintains a record of all allowable COMSEC material that has been issued on a hand receipt for removal from the crypto-center;
 - (10) Maintains Regular COMSEC Record (RCR) files, and a COMSEC material record system (either COMSEC material record cards or PC-based system) for all COMSEC material charged to the account. If a PC-based system is used, all information requested on the COMSEC material record card must be included;
 - (11) Prepares and submits such COMSEC material transfer, inventory, and destruction reports;
 - (12) Performs the additional functions applicable when the COMSEC Custodian is accountable to the DOE COMSEC Control Officer for TS COMSEC material;
 - (13) Maintains records of cryptographic and COMSEC access/termination briefings;
 - (14) Ensures control of and accountability for all Tamper Indicating Prismatic Seals (TIPS) issued to a site;
 - (15) Oversees keying and operation of crypto-equipment charged to the account; and
 - (16) Attends formal DOE COR COMSEC training once every four (4) years.
- d. Alternate COMSEC Custodian. This individual is a Federal employee or contractor responsible for assisting the COMSEC Custodian in the duties listed above. During periods when the COMSEC Custodian is unavailable, the Alternate COMSEC Custodian is authorized and required to perform these duties. The DOE COR requires that a primary Alternate COMSEC Custodian be indentified on the account appointment memorandum. The primary Alternate COMSEC Custodian must attend the formal training once every four years and be able to do all the require functions of the Custodian position.
- e. Crypto-operator. This individual is a Federal employee or contractor responsible for using crypto-materials to encrypt, decrypt, or authenticate information. Crypto-operators require access to classified cryptographic information, written assignment to perform cryptographic operations, and specific authority for access to TS COMSEC material if applicable. The duties of a Crypto-operator are very limited within the COMSEC Program. The only duties are related to crypto-equipment operations; this individual has no role in any of the other Telecommunications Security Programs. This individual:

- (1) Prepares COMSEC equipment, cryptographic keying material, and related telecommunications equipment for operation, and operates crypto-equipment in accordance with appropriate operating instructions;
- (2) Prepares, encrypts, and transmits outgoing messages and receives, decrypts, edits, and places appropriate marking on incoming messages;
- (3) Posts records, files message copies, safeguards, and accounts for keying material;
- (4) Maintains familiarity with and applies applicable KAM and KAO crypto-procedures, DOE communication security instructions, and local crypto-center practices; and
- (5) Notifies the cognizant COMSEC Custodian or COMSEC Control Officer of all reportable cryptographic occurrences that the operator observes or suspects.

3. DOE Emissions (TEMPEST) Program

- a. TEMPEST Coordinator. The TEMPEST Coordinator position is not identified in National policy. This position was created by DOE and only exists within the DOE TEMPEST Program.
 - (1) A TEMPEST Coordinator, designated in writing to the DOE CTTA Office, must be a DOE Federal employee, contractor, or subcontractor who is knowledgeable concerning the requirements of this Order and *Attachment 5, Classified Technical Section*.
 - (2) The TEMPEST Coordinator for all Headquarters elements is the DOE CTTA.
 - (3) It is required that the TEMPEST Coordinator or a designated Alternate attend the annual DOE Telecommunications Security Workshop at least once every four years for accomplishing his/her duties and to acquire new information concerning the TEMPEST Program.
 - (4) TEMPEST Coordinator Responsibilities
 - (a) When the TEMPEST Coordinator has determined that a location requires protection under the TEMPEST Program, he/she must refer to the criteria in this CRD and recommend countermeasures that will be noted in the TEMPEST plan. The completed TEMPEST plan must be forwarded to the DOE CTTA for review and approval. DOE CTTA approved TEMPEST plans become site

specific standards that serve as the basis for program audits, reviews, and/or inspections.

- (b) Each TEMPEST Coordinator must conduct a TEMPEST threat assessment, special review and an indices review annually to ensure that the TEMPEST posture has not changed. If no changes have occurred, the TEMPEST plan need not be revised but a memorandum must be forwarded to the DOE CTTA indicating the TEMPEST threat assessment, special review, and indices review were conducted and there are no changes. The memorandum response (indicating concurrence from the DOE CTTA) that the TEMPEST Coordinator receives from the DOE CTTA must be attached to the TEMPEST plan.
 - (c) A TEMPEST Coordinator is responsible for conducting an initial special review and conducting special reviews annually to ensure that the TEMPEST posture has not changed.
 - (d) The TEMPEST Coordinator has the responsibility for maintaining the RED/BLACK requirements and electronic emanations security for the facility based on the TEMPEST threat assessment and the specific countermeasures that have been approved by the DOE CTTA for the facility.
- (5) The DOE SAP Program Manager and the DOE CTTA have agreed that all SAP Security Coordinators will allow their site TEMPEST Coordinator to conduct a TEMPEST threat assessment and a special review; and to prepare a TEMPEST plan for each SAP (it makes no difference whether the SAP is acknowledged or unacknowledged) at the site. Due to security, classification, and Operations Security (OPSEC) requirements, all SAP areas will be protected, reviewed, and identified as TS. The SAP Security Coordinator will not be divulging to the TEMPEST Coordinator that the area where the TEMPEST threat assessment is being conducted actually contains SAP information.

4. DOE Protective Distribution System Program

- a. Protected Transmission System (PTS) Approval Authority. The PTSAA or designee at the cognizant DOE office must approve a PDS plan. The user site must install the PDS (for a new PDS installation it is required that the design of the PDS be approved by the PTSAA or designee before it is installed) in accordance with the PDS plan. The PDS must be inspected by the PTSAA or designee to verify compliance with the plan prior to transmission of classified information. The TSPM is the PTSAA for DOE Headquarters.
- b. Protected Transmission System Coordinator. A DOE Federal or contractor employee, appointed by site management and designated in writing to the site

PTSAA or designee, who will notify the DOE TSPM in writing of the designation. This individual must have knowledge concerning the installation, maintenance, and inspection of Protected Transmission Systems as defined in this Order.

- c. Alternate Protected Transmission System Coordinator. A DOE Federal or contractor employee, appointed by site management and designated in writing to the site PTSAA or designee, who will notify the DOE TSPM in writing of the designation. The Alternate PTS Coordinator will assist the PTS Coordinator in the installation, maintenance, and inspection of Protect Transmission Systems as defined in this Order.
- d. PTS Inspector. A DOE Federal or contractor employee, appointed by site management and designated in writing to the site PTSAA or designee, who will notify the DOE TSPM in writing of the designation. This individual will provide assistance in conducting technical and/or visual inspections for the site PDS Program.

The duties of a PTS Inspector are very limited within the PDS Program. The only duty is to assist with the PDS inspections. This individual has no role in any of the other Telecommunications Security Programs. PTS Inspector is only authorized to receive applicable subject matter for the performance of the assigned duties.

DEVIATION APPROVAL PROCESS

Telecommunications Security Program Deviations Matrix

	COMSEC	TEMPEST	PDS
Equivalency (a.k.a variance)		✓	✓
Exemption (a.k.a waiver, exception)	✓	✓	✓

1. EQUIVALENCY

- a. COMSEC. Equivalencies are not allowed in the COMSEC Program.
- b. TEMPEST. If a site has a TEMPEST plan or Transmission Security memorandum, an amendment reflecting the equivalency will be prepared and forwarded through the cognizant TSOM to the DOE CTTA for review and approval or disapproval.
- c. Protected Distribution Systems (PDS). If a site has a PDS plan, an amendment reflecting the equivalency will be prepared and approved by the site PTSAA or designee with written notification provided to the cognizant TSOM. The PTSAA or designee approved amendment must be available for the PDS program review conducted by the responsible DOE Headquarters representatives.
- d. An equivalency may be written in the body of an initial TEMPEST plan, Transmission Security memorandum or PDS plan but it must be noted as an equivalency and be approved by the proper approval authorities.

2. EXEMPTION

- a. COMSEC. A request for an exemption within the COMSEC Program must be submitted to the cognizant TSOM and then forwarded to the DOE COR Manager for review and approval. Exemptions within the COMSEC Program that address extended hand receipts, unique storage or access requirements, extended crypto-periods, etc., are considered by the DOE COR Manager when a COMSEC account must support unique operating requirements and environments. When approvals are issued for these requests, the length of the authorized exemption will be identified within the memorandum.
- b. TEMPEST. An exemption is granted only when correction of a nonstandard condition is judged to be non-feasible and compensatory measures are inadequate to preclude the acceptance of risk. If a site has a TEMPEST plan or Transmission Security memorandum, an amendment reflecting the exemption will be prepared and

forwarded through the cognizant TSOM to the DOE CTTA for review and approval or disapproval.

- c. PDS. If a site has a PDS plan, an amendment reflecting the exemption will be prepared and approved by the site PTSAA or designee with written notification provided to the cognizant TSOM. All PTSAA or designee approved exemptions must be available for the PDS program review conducted by the responsible DOE Headquarters program review representatives.
- d. All requests for exemption approvals must be coordinated with the local Office of Security before final approval may be granted. Exemptions may be granted for a period of up to 1 year. All approved exemptions will be annually reviewed for renewal purposes by the DOE CTTA, PTSAA, or designee. Requests for continuation of exemptions, including justification, are submitted for approval whenever a major change in site safeguards and security configuration or mission offers an opportunity for corrective action to terminate the nonstandard condition. Exemptions must be documented.

3. OTHER REQUIREMENTS

- a. Compensatory measures that have been implemented and are used to form the basis for an equivalency or exemption request are subject to formal vulnerability assessments and must be performance tested and validated by the site DOE TSOM. The results of the vulnerability assessment and performance test must be documented and forwarded to the TSPM for review. All documentation for vulnerability assessment and performance testing for a PDS must be made available to the responsible DOE Headquarters representatives during a PDS program review. Performance testing and documentation may be required for locally approved equivalencies as well.
- b. On-site reviews, assessments, and validation tests may be performed to obtain a full understanding of the nature and impact of an approved deviation. This can lead to a reversal of any deviation approval if, in the judgment of the cognizant Security Office, DOE TSPM, or site PTSAA or designee, adequate protection is not being provided or the deviation request is not justified.

REFERENCES

APPLICABILITY. This Attachment provides information and/or requirements associated with DOE O 205.2 as well as information and/or requirements applicable to contracts in which the associated CRD (*Attachment 1* to DOE O 205.2) is inserted. The Attachment applies to DOE Federal employees and contractors.

1. National Policy and Directives. Issuances of the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), Policies (P), Directives (D), and Instructions (I).
 - a. National Agency Communications Security Information Memorandum No. 5000, *TEMPEST Fundamentals*, dated 1 Feb 1982.
 - b. COMSEC 1-93, *Nomenclature for Communications Security Material*, dated 14 October 1993.
 - c. CNSSP No. 3, *National Policy on Granting Access to U.S. Classified Cryptographic Information*, dated October 2007.
 - d. CNSSP No. 17, *Policy on Wireless Communication*, dated May 2010.
 - e. CNSSP No. 300, *National Policy on Control of Compromising Emanations*, dated April 2004.
 - f. NSTISS/TEMPEST 1-95, *Shielded Enclosures*, dated 30 Jan 95.
 - g. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4001, *Controlled Cryptographic Items*, dated July 1996.
 - h. NSTISSI No. 4003, *Reporting and Evaluating COMSEC Incidents*, dated 02 December 1991.
 - i. NSTISSI No. 4004.1, *Destruction and Emergency Protection Procedures for COMSEC and Classified Material w/amended ANNEX B dated 9 Jan 08*, dated August 2006.
 - j. NSTISSI No. 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials*, dated August 1997.
 - k. NSTISSI No. 4031, *Cryptographic High Value Products*, dated 2011.
 - l. NSTISSI No. 7000, *TEMPEST Countermeasures for Facilities*, dated 29 November 1993.
 - m. NSTISSI No. 7001, *NONSTOP Countermeasures*, dated 15 June 1994.
 - n. NSTISSI No.7003, *Protective Distribution Systems (PDS)*, dated 13 December 1996.

- o. NSTISSAM TEMPEST/2-95, *RED/BLACK Installation Guidance*, dated 12 December 1995.

2. DOE Orders, Manuals, Notices, and Guidelines

- a. DOE M 470.4-2A, *Physical Protection*, dated 7-23-09.
- b. DOE O 205.1B, *Draft Department of Energy Cyber Security Program*, dated 2011.
- c. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 3-01-10.
- d. *DOE Communication Security (COMSEC) Program Supplemental Guide - Draft*, dated 2011.
- e. *DOE Emissions (TEMPEST) Program Supplemental Guide - Draft*, dated 2011.
- f. *DOE Protected Transmission Systems (PTS) Program Supplemental Guide -Draft* dated 2011.

3. Other.

- a. Department of Defense (DOD) Military Handbook-419A, *Grounding Bonding & Shielding For Electronic Equipment and Facilities*, dated 29 December 1987.
- b. DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, dated February 2006.
- c. Executive Order 12344, "*Navel Nuclear Propulsion Program*", dated 2-1-82.
- d. National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication (Pub) 140-2, *Security Requirements for Cryptographic Modules*, dated: May 2001.
- e. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated December 2004.
- f. United States Code/Title 18/Part I/Chapter 37/Section 798, *Disclosures of Classified Information*.

Classified Technical Section

For distribution, please contact the DOE Telecommunications Security Program Manager at 301-903-3957.