U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 470.6

Approved: 9-2-2015
Chg 1 (MinChg): 1-11-2017

SUBJECT: TECHNICAL SECURITY PROGRAM

1. PURPOSE.

This Order implements the Department of Energy (DOE) Technical Security Program (TSP). This program represents the convergence of two distinct disciplines: Counterintelligence (CI) and Security Countermeasures.

The elements of the TSP are driven by national level, interagency programs that are codified in various laws, Executive Orders, national polices and directives.

The scope of the DOE TSP is the following elements:

a. Technical Surveillance Countermeasures (TSCM) - designed to detect, deter, isolate, and nullify technical surveillance penetrations and technical security hazards.

b. TEMPEST - designed to prevent the unauthorized intercept of compromising emanations that may be present in information processing communication equipment, systems, and components.

c. Protected Distribution Systems (PDS) - designed to protect unencrypted classified signal/data lines that exit secure areas and traverse through areas of lesser security.

d. Wireless Security (WISEC) - designed to test/evaluate the impact of mobile and fixed wireless communication devices used in or near classified and sensitive unclassified activity areas for the purpose of determining risks and countermeasures.

e. Communications Security (COMSEC) - designed to protect and control the means and materials used to provide encrypted communications.

2. CANCELLATIONS.

a. DOE M 470.4-4A Chg. 1, *Information Security Manual*, dated 10-12-2010, Section D – Technical Surveillance Countermeasures (Official Use Only) and classified annex (Secret).

b. DOE M 205.1-3, *Telecommunications Security Manual* (Official Use Only) and Part II (Secret), dated 4-17-2006 to include classified annexes.

c. 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 (CRD) 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of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

a. All Departmental Elements. Except for the equivalencies/exemptions in paragraph 3.f., this Order applies to all Departmental Elements. The Administrator, National Nuclear Security Administration (NNSA), must ensure that NNSA employees comply with their responsibilities under this Order. Nothing in this Order will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of the National Nuclear Security Administration Act (NNSA Act,50 U.S.C. § 2402(d)) and section 3212(d) of Public Law (P.L.) 106-65, National Defense Authorization Act for Fiscal Year (FY) 2000, to establish Administration-specific policies, unless disapproved by the Secretary.

b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.f, the CRD, Attachment 1, sets forth requirements of this Order that will apply to contracts that include the CRD. The CRD must be included in contracts that involve classified information, and be evaluated for inclusion in contracts that involve Sensitive but Unclassified (SBU)/Controlled Unclassified Information (CUI).

c. This Order applies to the Bonneville Power Administration (BPA). The BPA Administrator will assure that BPA employees and contractors comply with their respective responsibilities under this directive consistent with BPA's self-financing, procurement and other statutory authorities.

d. The requirements in this Order apply to DOE (and DOE contractor) activities and facilities that are subject to licensing and related regulatory authority or certification by the Nuclear Regulatory Commission (NRC). The requirements in this Order should be applied consistent with Executive Order (E.O.) 12829, "Executive National Industrial Security Program" (January 6, 1993), the 1996 "Memorandum of Understanding Between the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission Under the Provisions of the National Industrial Security Program" as may be amended or superseded, and related memoranda of understanding between NRC and DOE concerning classified information, executed in accordance with applicable laws, regulations, policies, directives, and requirements.

e. In accordance with the responsibilities and authorities assigned by E.O. Order 12344, Naval Nuclear Propulsion Program (February 1, 1982), 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.

f. Equivalencies/Exemptions for DOE O 470.6.

Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1C, *Departmental Directive Program*.

Requests for equivalencies or exemptions from the requirements in this Order must be supported by a Technical Security Vulnerability Assessment (TSVA). The analysis must identify compensatory measures, if applicable, or alternative controls to be implemented. All approved equivalencies and exemptions under this Order must be entered in the Safeguards and Security Information Management System (SSIMS) database and incorporated into the affected security plan(s) except for Sensitive Compartmented Information Facilities (SCIF), Special Access Program Facilities (SAPF) and the information that falls under the authority of the Director of National Intelligence (DNI) or a Special Access Program (SAP) Manager. Equivalencies and exemptions become a valid basis for operation when they have been entered in SSIMS or approved by the Senior Intelligence Officer (SIO) or SAP Program Manager and documented in the appropriate security plan, and incorporated into site or facility procedures.

This Order's requirements are found in, or based on regulations issued by Federal agencies, laws, National Security Directives, Intelligence Community Issuances, Committee on National Security System (CNSS) Issuances, Code of Federal Regulations (CFR), Executive Orders, and Presidential Directives. In such cases, the process for deviating from requirements contained in the source document must be applied. If the source document does not include a deviation process, the DOE Office of the General Counsel or NNSA Office of General Counsel, if an NNSA element is involved, must be consulted to determine whether deviation from the source can be legally pursued. TSP Director review for concurrence or non-concurrence is required for both exemptions and equivalencies to this Order.

g. Relationship to DOE O 205.1B, *DOE Cyber Security Program*.

DOE Order 205.1B and DOE Order 470.6 complement each other in the security protections each Order addresses, both for the Cyber Security Program and the TSP as defined in each Order. Additionally, the Orders complement, and do not contradict, the delegations and authorities of the Chief Information Officer (CIO) and the Associate Under Secretary for Environment, Health, Safety and Security. A risk management approach is applicable for the implementation of cyber security and technical security, except for those requirements within the TSP that require compliance based on laws, regulations, Executive Orders, and other cognizant government agency Orders. When a deviation from a non-DOE requirement is identified, it must be resolved in accordance with the appropriate governing instruction. Inability to comply must be brought to the attention of the TSP Director and the appropriate authority such as the respective Program Secretarial Officer and CIO for matters involving cyber security.

4. REQUIREMENTS.

a. Only trained and certified individuals will conduct TSP operational program activities, such as TSCM services, TSP Reviews, COMSEC utilization determinations, or TEMPEST reviews in accordance with this Order and National Requirements.

b. Program offices must implement all elements included within this Order. This includes, but is not limited to, equipment, processes, training, personnel, and direction.

c. Information required by this Order relevant to the TSP and this Order must be maintained and, upon request, provided to the Director, TSP. Distribution of the classified TSP Annexes is limited to the TSP programmatic channels, their designees, or others as determined by the Director, TSP, based upon a need-to-know determination.

d. Access to TSP operational information and activities requires appropriate clearance, relevant access approval, and need-to-know. Distribution of Attachments 3, 4 and 5 of this Order is determined by the Director, TSP.

e. Methods to deter, detect, respond to, and mitigate unauthorized access to classified and sensitive unclassified information that conform with the requirements of this Order must be implemented.

f. Reciprocity requirements between departments and agencies in which reciprocal acceptance of interagency security policies and procedures is designed to reduce aggregate costs, promote interoperability of agency security systems, preserve the vitality of the U.S. industrial base, and advance national security objectives must be implemented.

g. Information requested by the TSP office must be provided as requested/required. Additional requirements for conducting and reporting service activities are found in the attachments to this Order. Distribution of the classified TSP Annex to Attachment 3 is limited to the Officially Designated Federal Security Authority (ODFSA), their designees, or others as determined by the Director, TSP, on a need-to-know basis.

5. RESPONSIBILITIES.

a. The Secretary of Energy.

Designates the Departmental Certified TEMPEST Technical Authority (DCTTA) pursuant to National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems.

b. The Administrator, NNSA.

(1) Ensures that an adequate number of qualified personnel and the appropriate equipment are available to effectively support the TSP mission requirements within the NNSA.

(2) At the request of the DOE TSP, provides access to NNSA inspection summary reports that provide the dates of inspections; descriptions of the facilities or spaces inspected; lists of hazards, vulnerabilities, and findings; and required corrective actions.

(3) NNSA must report any unauthorized electronic device or technology discovery, or suspect anomaly/potential compromise to the DOE TSP immediately.

(4) NNSA coordinates with DOE on any major change to the TSCM/TEMPEST programs or implementation.

c. Chief Security Officers.

Ensure that the requirements of this Order and its attachments are implemented for facilities, activities, or programs under their cognizance thru the Program Offices and ODFSAs.

d. Secretarial Officers.

Ensure that the requirements of this Order and its attachments are implemented for facilities, activities, or programs under their cognizance. Review, and where justified, approve requests for equivalencies and exemptions to the requirements of this Order, processed in accordance with DOE O 251.1C.

e. Associate Under Secretary for Environment, Health, Safety and Security.

(1) Is programmatically responsible for the DOE TSP elements for the Department.

(2) Designates the senior agency official responsible for directing, managing, providing oversight and administering the DOE TSP.

(3) Establishes and maintains an effective DOE TSP in accordance with national policy and reciprocity requirements.

(4) In coordination with the Heads of Field Elements, notifies contracting officers when DOE contractors are affected by this Order.

(5) Performs annual program reviews to evaluate ongoing activities; reviews future plans and projects, resource requirements and major concerns and issues.

f. Director, Office of Corporate Security Strategy, Analysis and Special Operations.

(1) Is functionally responsible for the DOE TSP elements for the Department.

(2) Will mediate any difference in professional opinion concerning TSP activities between elements.

g. Director, Technical Security Program.

(1) Provides Concurrence or Non-Concurrence to appropriate DOE organization/program office to conduct TSP services, acquire and possess TSP equipment, and to have TSCM/TEMPEST Service practitioners.

(2) Develops, coordinates, and interprets the Department's TSP policy consistent with strategies and reciprocity policies governing the protection of national security and other critical assets entrusted to the Department.

(3) Provides TSP services/functions for DOE Headquarters facilities and provides field assistance as necessary.

(4) Serves as the Central Office of Record (COR) for COMSEC accounting for DOE, including NNSA. Establishes and maintains a COMSEC Material Control System (CMCS) for the Department. Administers the activities of the DOE COR Manager.

(5) Controls usage and disposition of all COMSEC material used by DOE offices and DOE contractors when such material is used in conjunction with activities funded, contracted for, or otherwise arranged for by DOE.

(6) Coordinates with program offices regarding the release or disclosure of classified and sensitive unclassified TSP information.

(7) Represents DOE, including NNSA, on interagency policy coordinating committees and other technical support working groups and keeps TSP personnel informed of national and Departmental policy developments.

(8) Coordinates planning, selection, acquisition, use, and disposition of all cryptographic equipment, crypto-related equipment, authentication material, and algorithms approved for the protection of sensitive unclassified COMSEC information.

(9) Reviews the effectiveness and efficiency of DOE secure communications operations, and initiates recommendations or changes for improvement where necessary.

(10) Administers an on-site COMSEC audit and crypto-facility survey program pertaining to crypto-security, transmission security, and emissions security.

(11) Coordinates and approves interagency TSP activities

(12) Chairs the Process Implementation Working Group.

(13) Approves TSCM and TEMPEST specific training content, and coordinates with programs to ensure an enterprise approach to equipment procurement.

(14) Approves personnel who will conduct TSP operational activities such as TSCM services, TSP reviews, COMSEC utilization determinations or TEMPEST reviews.

(15) Assumes operational control of TSP activities during TSP security incidents as outlined in Attachment 4. If NNSA equities are involved, activities will be coordinated with the appropriate NNSA entity.

(16) Coordinate with DOE CIO on the development of TSP policy that directly or indirectly affects the implementation of departmental cyber policies.

(17) Alert CIOs and Authorizing Officials of potential impacts to cyber programs within sites that fall under TSP. Assist in developing remediation strategies consistent with federal law and departmental risk management strategies.

(18) Coordinates with CIOs to facilitate exchange of information specific to threats to information systems.

h. Director, Office of Intelligence and Counterintelligence.

(1) Acts as liaison, as requested by Director, TSP, with other agencies of the Intelligence Community on matters relevant to the TSP.

(2) Provides intelligence-related information concerning TSP programs to the Director, TSP.

(3) Conducts CI activities and provides CI for TSP activities.

(4) Ensures all Intelligence Work (IW) projects at the national laboratories comply with this directive to ensure reciprocity and protection of DOE information.

(5) Appoints a liaison responsible for coordinating implementation of TSP requirements with respect to SCIFs.

(6) Ensures that approved documentation for their programs, sites, facilities, and operations is developed, maintained, and provided to TSP personnel as necessary.

(7) Provides access to systems and areas under their control for TSP personnel to perform activities required in this Order.

(8) Grants all necessary access for program reviews, audits, inspections, surveys and/or inquiries.

(9) Serves as ODFSA for TSP requirements for all DOE SCIFs.

i. Office of the Chief Information Officer.

(1) The CIO recognizes intrinsic relationship between TSP and cyber and the need for increased security for systems under TSP. Any deviation from federal requirements will be handled in accordance with governing directives and in coordination through the appropriate Program Office. The roles and responsibilities of the DOE CIO are defined in DOE Order 205.1B.

(2) Coordinate with the TSP Director on the development of TSP policy that directly or indirectly affects the implementation of Departmental cyber policies.

(3) Develop Departmental response to potential cyber impacts to sites that fall under TSP. Assist appropriate Program Offices in developing remediation strategies consistent with federal law and Departmental risk management strategies.

(4) Coordinates with DOE TSP to facilitate exchange of information specific to threats to information systems.

(5) Represent the Department's cyber position as it relates to TSP. Any official representation or responses to Other Government Agencies (OGAs) on cyber issues related to CIO authorities must be coordinated through DOE CIO as applicable.

(6) Alerts Director TSP of potential cyber issues that may impact technical security and operations. Assist in developing remediation strategies consistent with federal regulation and departmental risk management strategies.

(7) Provides support to activities of the TSP required in this Order.

(8) Coordinates between TSP and OGAs for cyber related issues affecting TSP activities.

j. Heads of Field Elements and Offices.

(1) Are functionally responsible for the DOE TSP elements at locations under their cognizance.

(2) Designate Federal officials responsible for directing, managing, oversight and administering the TSP activities for their sites/areas of responsibility.

(3) Determine TSP staffing positions appropriate for locations under their cognizance and ensure necessary resources are available for an effective DOE TSP in accordance with national policy and reciprocity requirements and this Order.

(4) Designate a Federal Official/s responsible for implementation of TSP activities for their sites/areas of responsibility.

(5) Ensure annual program reviews are performed to evaluate ongoing activities; establish future plans and projects; determine resource requirements, including the resources necessary to implement and administer this Order and major concerns and issues.

(6) Will maintain a list of facilities requiring TSP services for the next FY to include the nature of the services needed.

(7) Will maintain a list of facilities that do not meet the minimum technical and physical security requirements as required by this Order.

(8) Will maintain Equivalency/Exemption documentation for facilities that will not receive requisite support, or do not meet the minimum technical and physical security requirements.

(9) Suspend or cancel the classified activities in facilities when notified of vulnerabilities that place classified information at risk. Ensure the expeditious implementation of effective mitigation strategies to prevent the loss, compromise or potential unauthorized disclosure of classified information.

(10) Will report the discovery of technical security hazards and technical penetrations to the Appropriate Headquarters (DOE and/or NNSA) TSCM Program Manager, or the Director, TSP, who will notify the appropriate program offices, including the Office of Counterintelligence and the Departmental element.

k. Delegation of Authority.

Each delegation must be documented in written form. It may be included in other security plans or documentation approved by or according to direction from the accountable principal. Each delegator remains responsible for the delegate's acts or omissions in carrying out the purpose of the delegation.

l. Contracting Officers.

Upon final approval, modify contracts to incorporate the CRD (attachment 1) and program-specific implementing instructions from NNSA and DOE program offices into those contracts that involve classified information, classified matter or nuclear materials and contain DEAR clause 952.204-2, titled Security Requirements.

6. DEFINITIONS. For purpose of this Order, the following definitions apply.

a. Access. In addition to physically accessing a room or facility, it is also the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

b. Cognizant Security Authority/Officer. An entity charged with responsibility for physical, technical, personnel, and information security affecting that organization. (Within DOE this is defined as the ODFSA. See definition for ODFSA).

c. Classified Information. Information regardless of form or characteristics which is classified by statute or Executive Order. Such information includes:

(1) Restricted Data (RD) or Formerly Restricted Data (FRD) classified by the Atomic Energy Act or Title 10, Code of Federal Regulations part 1045;

(2) Transclassified Foreign Nuclear Information (TFNI classified by the Atomic Energy Act), and

(3) National Security Information (NSI) classified by E.O. 13526 or prior E.O.

d. Classified Matter. Anything in physical form that contains or reveals classified information.

e. Compromising Emanations (CE). Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information system equipment. See TEMPEST.

f. Controlled Unclassified Information. Unclassified information that requires safeguarding and dissemination controls, to the extent consistent with applicable statutes, regulations and Government policies.

g. Critical Information. Specific facts about friendly (e.g., U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

h. Facility Technical Threat Assessment (FTTA). A weighted system for determining the need and priority of TSCM services. Its purpose is to identify potential targets and to quantify the overall effectiveness of the site or facility's protection strategy. This is accomplished by analyzing the site or facility's characteristics: the presence of sensitive or classified material; local and national threat assessments; protective force capabilities; and the presence of neutralization/countermeasures mitigations. The FTTA value helps the TSCMPM determine the number of sites and facilities that require services and the priority for their completion.

i. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

j. National Security System (NSS). Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency.

(1) the function, operation, or use of which:

(a) involves intelligence activities;

(b) involves cryptologic activities related to national security;

(c) involves command and control of military forces;

(d) involves equipment that is an integral part of a weapon or weapons system; or

(e) Is critical to the direct fulfillment of military or intelligence missions; or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(3) Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [44 U.S.C.3542(b)(2)]

k. Officially Designated Federal Security Authority. ODFSAs are Federal employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation. The ODFSA is charged with responsibility for physical, technical, personnel, and information security matters affecting the location identified in the delegation.

Delegation authority for these positions is originated according to direction from the accountable Undersecretary who also provides direction for further delegation of the ODFSA designations. Each delegation must be documented in written form. It may be included in other security plans or documentation approved by or according to direction from the accountable principal. Each delegator remains responsible for the delegate's acts or omissions in carrying out the purpose of the delegation. For sites with multiple ODFSAs, an ODFSA may redelegate responsibilities to a local TSCM Operations Manager (TSCMOM) provided all site ODFSAs agree to the redelegation.

l. Policy and Process Implementation Working Group. A DOE Working Group to develop procedures or guides as necessary to assist in implementation of this Order, and to review the Order periodically for necessary changes as technologies, laws, national policies, threats, or DOE policies are created or updated that affect the programs within the TSP.

m. System. Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

n. Technical Hazard. Any instance of information potentially leaving an area by unauthorized means due to equipment design or manufacture, damage, breakdown, configuration, or installation. All Hazards will be treated as penetrations until determined to be Hazards and categorized by the DOE TSP, in coordination with affected parties.

o. Technical Penetration. Any instance of information leaving an area by unauthorized technical means for monitoring by unauthorized entities, either through installation of a technical surveillance device, manipulation of software, interception and monitoring of fortuitous emanations, or intentional creation of a hazard.

p. Technical Security Vulnerability Assessment. Systematic examination of information systems, facilities, or products to determine the adequacy of technical and physical security measures, identify technical and security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

q. TEMPEST. A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

r. User. Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

s. Vulnerability Assessment (VA). A systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

7. REFERENCES. A list of references to assist in implementation of this Order provided as attachment 2.

8. CONTACT. For assistance regarding this directive, contact Director, DOE TSP, (301) 903-9992.

BY ORDER OF THE SECRETARY OF ENERGY:

ELIZABETH SHERWOOD-RANDALL
Deputy Secretary

TABLE OF CONTENTS

CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) established the (DOE) Technical Security Program (TSP) requirement for the Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors which process, discuss, and/or store classified national security information, restricted data, nuclear materials and/or sensitive but unclassified information.

Regardless of who performs the work, contractors must comply with the requirements of attachments 3 (including its Classified annex), 4 and 5 to DOE 470.6 referenced in and made part of this CRD and provide program requirements and information applicable to contracts in which this CRD is inserted.

Contractors must comply with applicable laws, regulations, policies, directives and other requirements as directed through contract by the NNSA or other DOE program office(s).

In performing work under this contract, the Contractor shall comply with the requirements of applicable federal, state, and local laws and regulations (including DOE regulations), unless relief has been granted in writing by the appropriate regulatory agency. A list of laws, regulations and references to assist in implementing this Order are identified in attachment 2 for informational purposes. Omission of any applicable law or regulation from attachment 2 does not affect the obligation of the Contractor to comply with such law or regulation pursuant to this Order.

Contractors must also comply with DOE program offices and NNSA direction provided through the contract.

Each contractor is responsible for disseminating (flowing down) the requirements to subcontractors at any tier to the extent necessary to ensure the contractor's and subcontractor's compliance with the requirements.

A violation of the provisions of the contract/CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR Part 824, Procedural Rules of the Assessment of Civil Penalties for Classified Information Security Violations.

Contractors which process, discuss, and/or store **ONLY** Sensitive but Unclassified (SBU) or Controlled Unclassified Information (CUI) as identified in the National Archives and Records Administration (NARA) CUI Registry, must develop and maintain a graded risk process and an assessment for the protection of SBU/CUI in accordance with the requirements of attachments, 3, 4 and 5 to DOE Order 470.6. The graded risk process and assessment must be available to the responsible ODFSA, upon request.

REFERENCES

1. PURPOSE:

   a. This attachment provides information for use in implementing the programs implemented by this Order.

   b. Implementation of this Order shall comply with the requirements of applicable Federal, State, and local laws and regulations (including DOE regulations), unless relief has been granted in writing by the appropriate regulatory agency.

   c. Omission of any applicable law or regulation from this attachment does not affect the obligation of to comply with current or future laws and regulations pursuant to this Order.

   d. A list of Other Government Requirements and Reference Information to assist in implementing the topics covered by this Order are identified in section 2 and 3.

   e. This attachment includes documents from various sources, each having differing conventions for denoting requirements. Federal and contractor personnel must consult the governing document system to determine the language used to distinguish requirements from recommended practices.

   f. Where the document system does not include such a description, common usage prevails. If a question arises regarding whether a specific provision is a requirement, contact the TSP Office for clarification.

   g. The documents listed within sections 2 and 3 should be construed to include any superseding issuance.

   h. This attachment only identifies unclassified, publicly releasable titles. Official Use Only (OUO) and Classified titled documents may be obtained by contacting the TSP.

2. OTHER GOVERNING REQUIREMENTS.

   a. This section provides a listing of documents that include requirements that are binding upon DOE personnel and contractors independent of this Order.

   b. This section also includes related Departmental Directives which are binding upon Federal personnel as specified in their applicability sections, and are binding upon contractors when their CRDs are included in the contract.

   c. This section also includes public laws, Executive Orders, and issuances of the governing security authorities that serve as conditions for the use of the security systems that DOE employs. These requirements are made mandatory for DOE Federal and Contractor personnel by means other than this Order and must be followed when implementing the requirements of this Order.

d. Committee on National Security Systems (CNSS) issuances are directed at those entities that own and/or are users of national security systems. The Heads of the Executive Departments and Agencies are responsible for ensuring that CNSS policies and directives are implemented within their departments or agencies. CNSS instructions provide guidance and technical criteria for specific Information Assurance (IA) issues. Contractors supporting the Executive Departments and Agencies are required to protect National Security Systems consistent with the CNSS requirements.

(1) CNSS Policies address national security systems issues from a broad perspective. They establish national-level goals and objectives, all of which are binding upon all U.S. Government departments and agencies.

(2) CNSS Directives address national security systems issues that go beyond the general policy documented under CNSS the policies topic. These directives provide details for achieving CNSS policies and are binding upon all U.S. Government departments and agencies.

(3) CNSS Instructions provide guidance and establish technical criteria for specific national security systems issues. These instructions include technical or implementation guidelines, restrictions, doctrines, and procedures applicable to information assurance. All instructions are binding upon all U.S. Government departments and agencies.

e. Listing.

(1) Public Laws (P.L.):

(a) P.L 108–458 - Intelligence Reform and Terrorism Prevention Act of 2004, December 17, 2004.

(b) P.L 107-347 - E-Government Act, Title III - Federal Information Security Management Act (FISMA), December 2002.

(c) P.L 107-306 - Counterintelligence Enhancement Act of 2002, as Amended

(d) P.L. 106-65, National Defense Authorization Act for Fiscal Year 2000, Title XXXII, National Nuclear Security Administration, as amended.

(e) P.L. 104–294, Economic Espionage Act of 1996, October 11, 1996.

(f) P. L. 100-235, Computer Security Act of 1987.

(g) P.L. 83-703, Atomic Energy Act of 1954, as amended.

(h) P. L. 110–53. National Security Act of 1947, As Amended August 2007.

(i) United States Code (U.S.C): Title 18 - Crimes and Criminal Procedures - Chapters 37, 90, 119

(j) U.S.C.: Title 18 Chapters 798, Disclosure of Classified Information.

(k) U.S.C: Title 50 – War and National Defense – Chapters 4 a, 4b, 4c, 36, 42, 44

(l) U.S.C.: Title 50 Chapter 2426, Congressional Oversight of Special Access Programs.

(m) 5 Code of Federal Regulations (CFR), parts 731 and 752, Administrative Personnel.

(n) 10 CFR part 851, Worker Safety and Health Program.

(o) 32 CFR parts 148 and 149, National Defense, Sub Title A, Chapter 1

(p) 32 CFR parts 2001 and 2003, National Defense.

(q) 32 CFR parts 2004, National Industrial Security Program.

(2) Executive Orders issued by the President:

(a) Executive Order (E.O.) 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001.

(b) E.O. 13526, Classified National Security Information, December 2009.

(c) E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 2011.

(d) E. O. 13556, Controlled Unclassified Information, November 2010.

(e) E.O. 13284, Executive Order Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, January 23, 2003.

(f) E.O. 12829, National Industrial Security Program.

(g) Amended by E.O.12885, Amendment to Executive Order No. 12829.

(h) E.O. 12968, Access to Classified Information.

(i) E.O. 13462, President's Intelligence Advisory Board and Intelligence Oversight Board.

(j) E.O. 12333, United States Intelligence Activities. Amended by E.O. 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security. Amended by E.O. 13355, Strengthened Management of the Intelligence Community.

(3) Federal Policies:

(a) National Security Directive (NSD)-42, National Policy for the Security of National Security Telecommunications and Information Systems, July 1990

(b) NSD -47, Counterintelligence and Security Countermeasures, October 1990

(c) National Security Decision Directive (NSDD) 84, Safeguarding National Security Information, March 1983.

(d) NSDD 298, National Operations Security Program, January 1988.

(e) National Industrial Security Program Operating Manual, February 2006 with Change 1, March 2013.

(f) National Industrial Security Program Operating Manual Supplement, 2006.

(g) NSDD 19, Protection of Classified National Security Council and Intelligence Information.

(h) Security Policy Board (SPB) Issuance 4-97, Reciprocity of Facilities National Policy on Reciprocity of Use and Inspections of Facilities.

(i) SPB Issuance 5-97, Guidelines for the Implementation and Oversight of the Use and Inspections of Facilities.

(j) SPB Issuance 6-97, National Policy on Technical Surveillance Countermeasures.

(k) SPB Procedural Guide 1-99, The Conduct of a TSCM Survey. (S)

(l) SPB Procedural Guide 2-99, Requirements for Reporting and Testing of TSCM Penetrations. (S)

(m) SPB Procedural Guide 3-99, Requirements for Reporting and Testing of Technical Hazards. (OUO)

(n) Presidential Decision Directive (PDD)/NSC 61, Energy Department Counterintelligence, February 1998. (C)

(o) PDD/NSC-63, Critical Infrastructure Protection, May 1998. (OUO)

(p) White House Memorandum, SUBJECT: Policies on Technical Surveillance Countermeasures and Reciprocity for Facilities, September 16, 1997.

(q) Physical Security Criteria for Federal Facilities, Interagency Security Committee Standard, April 12, 2010 (OUO)

(r) Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, February 2004.

(s) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

(t) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

(u) OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 2006.

(4) Intelligence Community (IC) issuances:

(a) IC Directive (ICD) 702 – Technical Surveillance Countermeasures, February 2008.

(b) ICD 703 – Protection of Classified National Intelligence, Including SCI, June 2013.

(c) ICD 700- Protection of National Intelligence, June 2012.

(d) ICD 705 - Sensitive Compartmented Information Facilities, May 2010.

(e) IC Standard (ICS) 705-1, Physical and Technical Standards for Sensitive Compartmented Information Facilities, Version 1.2, April 2012.

(f) ICS 705-2, Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities, September 2010.

(5) Department of Energy directives and classification guides:

(a) DOE O 470.4B, *Safeguards and Security Program*, dated 7-21-11.

(b) DOE O 471.6, *Information Security*, Admin Chg. 1, dated 6-29-11

(c) DOE O 473.3A, *Protection Program Operations*, dated 5-23-16.

(d) DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.

(e) DOE O 471.5, *Special Access Programs*, dated 3-29-11.

(f) DOE O 205.1B, *DOE Cyber Security Program*, dated 5-16-11.

(g) DOE O 481.1D, *Strategic Partnership Projects [Formerly Known as Work for Others (Non-Department of Energy Funded Work)]*, dated 12-5-16.

(h) DOE O 484.1, *Reimbursable Work for Department of Homeland Security*, March 2011.

(i) CG-TSCM-1, DOE, TSCM Classification Guide (S/NSI).

(j) CG-SS-4, Classification and UCNI Guide for Safeguard and Security Information. (OUO).

(k) CG-SS-4A, DOE Safeguard and Security Classification Guide (S/NSI).

(l) DOE Sensitive Compartmented Facilities Manual.

(6) National Institute of Standards and Technology (NIST) issuances:

(a) NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.

(b) NIST SP 800-124r1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013.

(c) NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs), February 2012.

(d) NIST SP 800-127, Guide to Securing WiMAX Wireless Communications, September 2010.

(e) NIST SP 800-124 Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013.

(f) NIST SP 800-121 Rev. 1, Guide to Bluetooth Security, June 2012.

(g) NIST SP 800-101, Guidelines on Cell Phone Forensics, May 2007.

(h) NIST SP 800-72, Guidelines on PDA Forensics, November 2004.

(i) NIST SP 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.

(j) NIST SP 800-124, Guidelines on Cell Phone and PDA Security, October 2008.

(k) NIST SP 800-58, Security Considerations for Voice over IP Systems, January 2005.

(l) NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

(7) Committee on National Security Systems (CNSS). Issuances from this Federal entity:

(a) Committee on National Security Systems (CNSS) Index of National Security Systems Issuance, June 2013.

(b) CNSS Policies (P):

1 CNSSP 1, National Policy for Safeguarding and Control of COMSEC Materials, September 2004.

2 CNSSP 3, National Policy for Granting Access to U.S. Classified Cryptographic Information, October 2007.

3 CNSSP 8, Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations, August 2012. (OUO)

4 CNSSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, June 2013.

5 CNSSP 12, National Information Assurance Policy for Space Systems used to Support National Security Systems, November 28, 2012.

6 CNSSP 14, National Policy Governing the Release of Information Assurance (IA) Products and Services to Authorized U.S. Activities that are not a Part of the Federal Government, November 2002.

7 CNSSP 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, March 2010. (OUO)

8 CNSSP 16, National Policy for the Destruction of COMSEC Paper Material, October 2002. (OUO)

9 CNSSP 17, Policy on Wireless Systems, January 2014 (supersedes the CNSSP No. 17, National Information Assurance (IA) Policy on Wireless Capabilities, May 2010). (U)

10 CNSSP 18, National Policy on Classified Information Spillage, July 2006.

11 CNSSP 19, National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products, June 10, 2013.

12 CNSSP 21, National Information Assurance Policy on Enterprise Architectures for National Security Systems, Mar 2007.

13 CNSSP 22, Policy for Information Assurance Risk Management for National Security Systems, January 2012.

14 CNSSP 24, Policy on Assured Information Sharing (AIS for National Security Systems (NSS), May 2010.

15 CNSSP 25, National Policy for Public Key Infrastructure in National Security Systems, April 2009.

16 CNSSP 26, National Policy on Reducing the Risk of Removable Media, November 2010.

17 CNSSP 101, National Security Telecommunications and Information Systems Security (NSTISS) National Policy on Securing Voice Communications, September 14, 1999.

18 CNSSP 200, National Policy on Controlled Access Protection, July 15, 1987.

19 CNSSP 300, National Policy on Control of Compromising Emanations, April 2004. (OUO)

(c) CNSS Directives (D):

1 CNSS Directive (D) 500, Information Assurance (IA) Education, Training, and Awareness, August 2006.

2 CNSSD 501, NSTISS National Training Program for Information Systems Security (INFOSEC) Professionals, November 1992.

3 CNSSD 502, National Directive on Security of National Security Systems, December 2004.

4 CNSSD 504, Directive on Protecting National Security Systems from Insider Threat, February 4, 2014. (U)

5 CNSSD 505, Supply Chain Risk Management (SCRM), March 7, 2012. (OUO)

6 CNSSD 506, Directive to Implement PKI for the Protection of Systems Operating on Secret Level Networks, October 9, 2012.

7 CNSSD 600, NSTISS Communications Security (COMSEC) Monitoring, April 1990. (OUO)

8 CNSSD 900, Governing Procedures of the Committee on National Security Systems, May, 1 2013.

9 CNSSD 901, Committee on National Security Systems Issuance System, October 2012.

10 CNSSD 2005, (NACSI) Communications Security (COMSEC) End Item Modification, May, 28 1981. (OUO)

11 CNSSD 6001, (NACSI) Foreign Military Sales of Communications Security Articles and Services to Foreign Governments and International Organizations, September 21, 19 84. (C)

12 CNSSD 6002, (NACSI) Protection of Government Contractor Telecommunications, June 04, 1984.

13 CNSSD 8105, (NACSI) Operational Doctrine for TSEC/KG-45 (SANCHEZ), 16 December 16, 1980. (S)

14 CNSSD 8116, (NACSI) Operational Doctrine for the TSEC/CI-10 (ELWELL II), February 1, 1993. (C)

(d) CNSSI Instructions (I):

1 CNSSI 1300, Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy, Version 1.1, June 2011.

2 CNSSI 3000, (NTISS) Security Doctrine for the TSEC/KW-46 Fleet Broadcast System, April 4, 1986. (C)

3 CNSSI 3001, (NTISS) Operational Security Doctrine for the Automanual (AMS), October 30, 1989. (C)

4 CNSSI 3002, (NTISS) Operational Doctrine for the KGV-9 Removable Key Stream Generator Module, September 5, 1986. (OUO)

5 CNSSI 3003, (NSTISS) Operational Security Doctrine for the KG-66/KG- 66A/SO-66/KGR-66/KGV-68/KGR-68/KGV-68B, August 2000. (OUO)

6 CNSSI 3006, (NSTISS) (U) Operational Security Doctrine for the NAVSTAR Global Position System (GPS) Precise Positioning Service (PPS) User Segment Equipment, August 2001. (OUO)

7 CNSSI 3008, (NTISS) Operational Security Doctrine for Type I Communications Equipment Containing the FASCINATOR Secure Voice Module (SVM), May 1, 1989. (OUO)

8 CNSSI 3010, (NTISS) Operational Security Doctrine for the KY- 65A/75A, July 19, 1989. (S/NF)

9 CNSSI 3011, (NTISS) Operational Security Doctrine for KY-57/58, KY- 67 & KYV-2/2A, October 13, 1989. (OUO)

10 CNSSI 3012, (NTISS) Operational Security Doctrine for the KY-71, 27 November 1989. (OUO)

11 CNSSI 3013, (NTISS) Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type I Terminal, February 8, 1990. (OUO)

12 Annex E, System Security Guidance for the Motorola Vehicular-Mounted STU-III Cellular Telephone (Type 1), February 22, 1991. (OUO)

13 Annex F, Supplemental Operational Security Doctrine for the STU-III/A Terminal (Type 1), February 22, 1991. (OUO)

14 Annex G, System Security Guidance for the AT&T STU-III Access Control System (SACS) (Type 1), February 22, 1991. (OUO)

15 Annex H, STU-III Data Port Guidance, November 27, 1991. (OUO)

16 CNSSI 3014, (NSTISS) Management of Off-Line Cryptosystems, February 1, 1991. (OUO)

17 CNSSI 3015, (NSTISS) Operational Security Doctrine for the Fiber Alarmed Modem (FAM)-131 Intrusion Detection Optical Communications System (IDOCS), February 28, 1991. (OUO)

18 CNSSI 3016, (NSTISS) Operational Security Doctrine for GILLAROO Personal Computer Security Device (PCSD), July 2, 1991. (OUO)

19 CNSSI 3017, (NSTISS), Operational Security Doctrine for Non-TRI-TAC KG-84A, KG-84C, KIV-7, and KIV-7HS, KIV-7HSA, and KIV-7HSB, March 2003. (C)

20 CNSSI 3018, (NSTISS) Operational Security Doctrine for the GUARDSMAN 100 and 100T, January 8, 1992. (OUO)

21 CNSSI 3019, (NSTISS) Operational Security Doctrine for the FASTLANE (KG-075 and KG-75A), October 30, 2001. (OUO)

22 CNSSI 3020, (NSTISS) Operational Security Doctrine for the KL-51 (RACE), February 11, 1992. (OUO)

23 CNSSI 3021, Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device (DTD), September 2002. (OUO)

24 CNSSI 3022, (NSTISS) Operational Security Doctrine for Trunk Encryption Devices (TEDs) KG-81, KG-94 Family, KG-95 Family, KG- 194 Family, and KIV-19 in Stand-Alone Applications, July 1999. (OUO)

25 CNSSI 3024, (NSTISS) (U) Operational Security Doctrine for KG-189 Strategic Trunk Encryptor, January 2000. (OUO)

26 CNSSI 3025, (NSTISS) Operational Security Doctrine for CIPHERTAC 2000 (CTAC 2000), August 1999. (OUO)

27 CNSSI 3026, (NSTISS) Operational Security Doctrine for the Motorola Network Encryption System (NES), April 1999. (OUO)

28 CNSSI 3028, (NSTISS) Operational Security Doctrine for the FORTEZZA User PCMCIA Card, December 2001. (U)

29 CNSSI 3029, Operational Systems Security Doctrine for TACLANE (KG- 175), May 2004. (OUO)

30 CNSS-089-04, Changes for CNSS Instruction No. 3029, August 25, 2004 (OUO)

31 CNSS-057-06, Changes for CNSS Instruction No. 3029, April 19, 2006 (OUO)

32 CNSSI 3030, (NSTISS) Operational Systems Security Doctrine for the FORTEZZA PLUS (KOV-14) and Cryptographic Card and Associated Secure Terminal Equipment (STE), October 26, 2001. (OUO)

33 CNSS-165-06, Amendment to NSTISSI No. 3030, October 20, 2006. (OUO)

34 CNSSI 3031, Operational Systems Security Doctrine for the SecteraTM In-Line Network Encryptor (KG-235), February 2003. (OUO)

35 CNSSI 3032, Operational Security Doctrine for the VIASAT Internet Protocol (VIP) Crypto Version 1 (KIV-21), August 2003. (OUO)

36 CNSSI 3034, Operational Security Doctrine for the SECNET TM 11 Wireless Local Area Network Interface Card, April 2004. (OUO)

37 CNSSI 3035, (CNSS) Operational Security Doctrine for the REDEAGLE KG-245 In-Line Network Encryptor (INE), March 2007. (OUO)

38 CNSSI 4000, Maintenance of Communications Security (COMSEC) Equipment, October 12, 2012. (OUO)

39 CNSSI 4001, Controlled Cryptographic Items, 7 May 7, 2013. (OUO)

40 CNSSI 4002, Classification Guide for COMSEC Information, June 5, 1986. (S/NF)

41 CNSS-066-04 authorizes pen & ink changes for NTISSI 4002, 2 July 2, 2004. (OUO)

42 CNSS-129-06 authorizes pen & ink changes for NTISSI 4002, November 2006. (OUO)

43 CNSS-054-09 authorizes pen & ink changes for NTISSI 4002, July 2009. (OUO)

44 CNSS-015-10 authorizes pen & ink changes for NTISSI 4002, March 2010. (S/REL)

45 CNSSI 4003, (NSTISS) Reporting and Evaluating COMSEC Incidents, December 2, 1991. (OUO)

46 CNSS-065-13 Amendment 1, April 26, 2013. (OUO)

47 CNSS-064-13 Addendum 1, April 26, 2013.

48 CNSSI 4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material w/amended ANNEX B (dated January 9, 2008), August 2006. (OUO)

49 CNSS-121-07 ANNEX B Amendment, August 2007. (OUO)

50 CNSSI 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 22, 2011. (OUO)

51 CNSSI 4006, Controlling Authorities for Traditional COMSEC Material, April 17, 2012. (OUO)

52 CNSSI 4007, COMSEC Utility Program, November 2007. (OUO)

53 CNSSI 4008, Program for the Management and Use of National Reserve Information Assurance Security Equipment, March 2007.

54 CNSSI 4009, National Information Assurance (IA) Glossary, April 2010.

55 CNSSI 4011, (NSTISS) National Training Standard for INFOSEC Professionals, June 20, 1994.

56 CNSSI 4031, Cryptographic High Value Products, February 16, 2012.

57 CNSSI 4032, Management and Use of Secure Data Network System (SDNS) FIREFLY Keying Material and Related Equipment, June 22, 2012. (OUO)

58 CNSSI 4033, Nomenclature for Communications Security Material, 14 November 14, 2012.

59 CNSSI 5000, Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony, April 2007.

60 CNSSI 5001, Type-Acceptance Program for Voice Over Internet Protocol (VOIP) Telephones, December 2007.

61 CNSSI 5002, National Information Assurance (IA) Instruction for Computerized Telephone Systems, February 24, 2012.

62 CNSSI 5006, National Instruction for Approved Telephone Equipment, September 2011.

63 CNSSI 5007, Telephone Security Equipment Submission and Evaluation Procedures, April 2013.

64 CNSSI 7000, TEMPEST Countermeasures for Facilities, May 2004. (C//REL)

65 CNSSI 7001, (NSTISS) NONSTOP Countermeasures, June 15, 1994. (S/NF)

66 CNSSI 7002, (NSTISS) TEMPEST Glossary, March 17, 1995. (S/NF)

67 CNSSI 7003, (NSTISS) Protected Distribution Systems (PDS), 13 December 13, 1996.

(e) Information Assurance Advisory Memoranda (IAAM):

1 IAAM, IA/01-12 NSA- Approved Commercial Solution Guidance, June 6, 2012.

2 IAAM, IA/01-07, IA Cryptographic Equipment Modernization Planning, August 2007. (S/REL)

3 IAAM, IA/01-04, Security Through Product Diversity, July 2004.

4 IAAM, IA/02-04, Retirement of Data Encryption Standard (DES) Based Cryptography to Protect National Security Systems, March 2005, Revised.

5 IAAM, IA/03-04, Advanced Encryption Standard (AES) Implementation, November 2004. (OUO)

(f) INFOSEC Advisory Memoranda (AM):

1 INFOSEC AM 1-00, (NSTISS) Use of the Federal Information Processing Standards (FIPS) 140-1 Validated Cryptographic Modules in Protecting Unclassified National Security Systems, February 8, 2000.

2 INFOSEC AM 2-00, (NSTISS) Strategy for Using the National Information Assurance Partnership (NIAP) for the Evaluation of Commercial Off-the- Shelf (COTS) Security Enabled Information Technology Products, February 8, 2000. (U)

(g) COMSEC Advisory Memoranda (AM):

1 COMSEC AM 1-85, Release of Communications Security Equipment, Material or Information to Foreign Enterprises, October 29, 1985.

2 COMSEC AM 1-87, TRI-TAC Keying Concepts, October 22, 1987. (C)

3 COMSEC AM 1-98, AN/CYZ-10/10A Data Transfer Device (DTD) Training, August 1998.

(h) NSTISS:

1 COMPUSEC AM 1-90, (NSTISS) Protection of Information Systems (IS) Outside the Continental United States (OCONUS), September 14, 1990. (OUO)

2 TEMPEST 2-91, (NSTISS) Compromising Emanations Analysis Handbook, 20 December 20, 1991. (C)

3 TEMPEST 1-92, (NSTISS) Compromising Emanations Laboratory Test Requirements, Electromagnetics, December 15, 1992. (C)

4 Appendix C of NSTISS AM TEMPEST/1-92 (U). (Issued via NSTISSC Memo, Serial: NSTISSC-002/94) January 19, 1994. (C)

5 Appendix E of NSTISS AM TEMPEST/1-92 (U). (Issued via NSTISSC Memo, Serial: NSTISSC-014/93) May 11, 1993.

6 Section 6 Change to NSTISS AM TEMPEST/1-92 (U) (Issued via NSTISSC Memo, Serial: NSTISSC-017/94) May 27, 1994. (OUO)

7 TEMPEST 2-92, (NSTISS) Procedures for TEMPEST Zoning, December 30, 1992. (OUO)

8 TEMPEST 1-93, (NSTISS) Compromising Emanations Field Test Requirements, Electromagnetics, August 30, 1993. (C)

9 TEMPEST 2-93, (NSTISS) Rationale for Compromising Emanations Laboratory and Field Test Requirements, Electromagnetics, October 14, 1993. (S)

10 Appendix J of NSTISS AM TEMPEST/2-93 (U). (Issued via NSTISSC Memo, Serial: NSTISSC-008/94) March 7, 1994. (C)

11 TEMPEST 1-95, (NSTISS) Shielded Enclosures, January 30, 1995. (OUO)

(i) TEMPEST:

1 TEMPEST 1-00, Maintenance and Disposition of TEMPEST Equipment, December 2000.

2 TEMPEST 01-02, Non-stop Evaluation Standard, October 2002. (C)

(j) CNSS:

1 CNSS AM TEMPEST 1-13 Red/Black Installation Guidance, January 2014 (supersedes NSTISSAM TEMPEST 2-95 and the TEMPEST 2-95 Addendum of February 2000). (U)

2 CNSS 4004, Communications Security Survey Guide, July 3, 1980. (C)

3 CNSS 5000, TEMPEST Fundamentals, February 1, 1982. (C)

4 CNSS 7002, (NACSEM) COMSEC Guidance for ADP Systems, September 1975. (C)

(k) Telecommunications Security Group (TSG) STANDARDS:

1 TSG STANDARD 1, Introduction to Telephone Security, March 1990.

2 TSG STANDARD 2, Guidelines for Computerized Telephone Systems, March 1990.

3 National Telecommunications Security Working Group (NTSWG) STANDARD 2a, Guidelines for Computerized Telephone Systems Supplemental, March 2001.

4 TSG STANDARD 3, Type-Acceptance Program for Telephones used with the Conventional Central Office Interface, March 1990.

5 TSG STANDARD 4, Type-Acceptance Program for Electronic Telephones used in Computerized Telephone Systems, March 1990.

6 TSG STANDARD 5, On-Hook Telephone Audio Security Performance Specification, March 1990.

(l) FED Standard 1037B, Telecommunications Glossary of

3. REFERENCE INFORMATION.

a. This section provides a documents and website that provide useful information, strategies, guidance, industry standards, best practices and policies.

b. These documents may not be binding requirements as standalone documents, but the documents maybe invoked as required to be utilized by other issuance in specific instances, such as Certified TEMPEST Technical Authority (CTTA) evaluations and testing requirements.

c. If not invoked within this Order or Other Governing Requirements, these documents should be considered and used as guides in the development of programs covered by this Order.

d. Although not invoked as requirements by this Order, deviations from these documents should be justified.

e. The listing of websites provides location where related information and some of the requirements documents associated with this Order may be located. These websites are provided to assist in locating information for implementation of the programs. The websites are not invoked as requirements by this Order.

f. Listing.

(1) Websites. The following tools and links may assist in locating unclassified DOE and national directives that have requirements that apply to this topical area. The documents provided within each tool may not be the official versions of the associated laws, policy and requirements documents, and directives. The current official version of any requirements directives must be used when developing policy or procedures. Links or references to the official documents or their websites are provided when available

(a) Department of Energy (DOE) Directives - https://www.directives.doe.gov/

(b) DOE Environment, Health, Safety and Security Safeguard and Security Policy Information Resource - https://pir.doe.gov/

(c) National Nuclear Security Administration (NNSA) Policy Information Resource - https://spr.energy.gov/

(d) National Institute of Standards and Technology (NIST) - http://www.nist.gov/publication-portal.cfm

(e) Committee on National Security Systems - https://www.cnss.gov/

(f) National Security Agency Information Assurance Directorate (NSA IAD) - https://www.iad.gov/iad/index.cfm

(g) National Archives - http://www.archives.gov/federal-register/ (Federal Laws, Executive Orders, Etc.)

(h) National Counterintelligence and Security Center (NCSC) - http://www.ncsc.gov/ (Counterintelligence and Security Issuances)

(i) Director of National Intelligence (DNI) Issuances - http://www.dni.gov/index.php/intelligence-community/ic-policies-reports (Intelligence Community Directives, Policies, etc.)

(j) Department of Defense (DOD) Issuances - http://www.dtic.mil/whs/directives/

NOTE: Documents on listed website may not contain the official or most current versions of the associated laws, policy and requirements documents, and directives. The current official version of any requirements documents must be used for implementing this Order.

(2) National Strategies:

(a) The National Technical Surveillance Countermeasures Strategy of the United States of America, 2008 (S/NF)

(b) The National Counterintelligence Strategy of the United States, 2009

(3) Department of Defense issuances:

(a) Joint Air Force - Army – Navy (JAFAN) Manuals, 6/0, 6/3, 6/4, 6/9

(b) Mil STD 188-124B, Grounding Bonding and Shielding, 1992. (OUO)

(c) Mil STE 461D Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility, August 1986. (OUO)

(4) National Security Agency Information Assurance Directorate (NSA/IAD) issuances:

(a) NSA/ IAD ADVISORY NO. IAA-001-2000, Security Guidance for Using Computers with Internal Microphones, February 2000 (OUO)

(b) NSA/IAD ADVISORY NO. IAA-00192: Secure Telephone Devices Used in Non Secure Environments, February 2002

(c) NSA/IAD ADVISORY NO. IAA-001-2000, Security Guidance for Using Computers with Internal Microphones, February 2000

(d) NSA/IAD ADVISORY NO. MA-005-2007, Video Teleconferencing Security Advisory, 17 August 2007

(e) Community Gold Standard for Information Assurance, Physical Hunting V1.1.1, July 2012

(f) Information Assurance Technical Framework (IATF) Document 3.1, Chapter 4, Technical Security Countermeasures, September 2002

(g) Technical Capabilities Report, May 2012 (S/NF/ORCON)

(h) NSA Specification - TEMPEST Testing requirements and limits, June 1993. (S)

(i) National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," August 5, 2005 (OUO)

(5) American Society for Testing and Materials (ASTM) issuances:

(a) ASTM International Classification E413 –Sounds Isolation

(b) ASTM Test Method E336 - Single-number ratings are field sound transmission class (FSTC), noise isolation class (NIC), and normalized noise isolation class (NNIC).

(c) ASTM Test Method E90 - The single-number rating is called sound transmission class (STC).

(d) ASTM Test Method E336 - Measurement of Airborne Sound Attenuation between Rooms in Buildings

(e) ASTM Test Method E596 -The single-number rating is called noise isolation class (NIC).

(6) Institute of Electrical and Electronics Engineers (IEEE) standard: IEEE Std C2-2012, National Electrical Safety Code, 2012.

(7) International Code Council code: International Code Council, International Building Code.

(8) National Fire Protection Association (NFPA) standards:

(a) NFPA 30, Flammable and Combustible Liquids Code, 2012.

(b) NFPA 70, National Electric Code, 2011.

ATTACHMENTS 3-5 (Official Use Only)

Available through Sam Soley: (301) 903-9992, sam.soley@hq.doe.gov.