DOE 5300.2D
5-18-92

THIS PAGE MUST BE KEPT WITH DOE 5300.2D, TELECOMMUNICATIONS; EMISSION SECURITY (TEMPEST)

DOE 5300.2D, TELECOMMUNICATIONS; EMISSION SECURITY (TEMPEST) HAS REVISED DOE 5300.2C TO REFLECT ORGANIZATIONAL, TITLE, ROUTING SYMBOL, AND OTHER EDITORIAL REVISIONS TO INCORPORATE CHANGES REQUIRED BY SEN-6. NO SUBSTANTIVE CHANGES HAVE BEEN MADE. DUE TO THE NUMBER OF PAGES AFFECTED BY THE REVISIONS, THE ORDER HAS BEEN ISSUED AS A REVISION.

U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5300.2D

5-18-92

SUBJECT: TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST)

1. PURPOSE. To establish the Department of Energy (DOE) emission security (TEMPEST) policy and program for automated information and telecommunications information processing equipment pursuant to national program requirements.

2. CANCELLATION. DOE 5300.2C, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST), of 12-19-89.

3. SCOPE. The provisions of this Order apply to all Departmental Elements and DOE contractors and subcontractors performing work for the Department as provided by law, and/or contract, and as implemented by the appropriate contracting officer.

4. REFERENCES.

   a. National Security Directive (NSD) 42, of 7-5-90, which establishes a national committee structure to protect classified information during electronic processing. Each operating agency of the Government must implement security standards pursuant to NSD-42.

   b. CG-SS-2, Safeguards and Security Classification Guide of 7-90, which provides guidance for classification of communications security (COMSEC) and TEMPEST information.

   c. DOE RED/BLACK Design Installation Guide, of 4-1-91, which provides technical TEMPEST RED/BLACK criteria for DOE and DOE contractor facilities.

   d. DOE 5300.1C, TELECOMMUNICATIONS, of 6-12-92, which establishes policy and general guidance for telecommunications services

   e. DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, of 1-29-88, which establishes uniform requirements policies, responsibilities, and procedures for the development and implementation of a DOE classified computer security program to ensure the security of classified information in automatic data processing (ADP) systems.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Information Resources Management

f. National Telecommunications and Information System Security Policy No. 300, of 10-3-88, "National Policy on Control of Compromising Emanations," which establishes United States Government policy for control of compromising emanations.

g. National Telecommunications and Information Systems Security Instructions No. 7000, "TEMPEST Countermeasures for Facilities," of 10-17-88, which provides minimal national guidance to determine the applicable TEMPEST countermeasures for equipment and facilities that process national security information.

5. DEFINITIONS.

a. COMSEC. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the result of such possessions and study. These measures involve proper application of cryptography, TEMPEST, physical, and transmission security standards.

b. Compromising Emanations or Emissions. Unintentional data-related or intelligence bearing signals which, if intercepted and analyzed, disclose the classified information being transmitted, received, handled, or otherwise processed by information processing equipment, systems, or components.

c. TEMPEST. The component of communications security that results from measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment, telecommunications, systems, and other classified information processing equipment.

d. TEMPEST. An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used interchangeably with the term "compromising emanations;" e.g., TEMPEST tests, TEMPEST inspections.

e. TEMPEST Control Zone. The contiguous space which surrounds the classified information processing equipment and its components that is under sufficient physical and technical control to preclude interception of compromising emanations. "Sufficient physical and technical control" means that security or other authorized personnel can exercise sufficient control over the space to prevent unauthorized persons from intercepting emissions that may be present within the zone. Government or contractor ownership of the space is not required.

f. Classified Information Processing Equipment. All electronic or electro-mechanical driven systems or components used to process information which has been classified under provision of

Executive Order 12356 or another proper authority. Also referred to as "automated information processing equipment."

6. POLICY. It is DOE policy to prevent the unauthorized intercept of compromising emanations that may be present in classified information processing communication equipment, systems, and components. To accomplish this:

   a. All classified information processing applications will be evaluated to determine what, if any, TEMPEST countermeasures are necessary.

   b. TEMPEST countermeasures will only be provided where required based on conducting an onsite threat and vulnerability analysis. Because of the high cost of installing and maintaining TEMPEST countermeasures, the evaluations will focus on threat and vulnerability analysis.

   c. The most economical TEMPEST countermeasure will be deployed for areas deemed threatened by hostile exploitations.

   d. No TEMPEST expenditure over $50,000 will be obligated without the written approval of the DOE Certified TEMPEST Technical Authority (CTTA). This limitation includes the costs associated with contractors or subcontractors hired to assist in the implementation of DOE TEMPEST programs.

   e. TEMPEST countermeasures will not be used for unclassified systems or components.

   f. A TEMPEST plan documenting the required elements of the site's TEMPEST program will be prepared by the cognizance authority.

7. RESPONSIBILITIES AND AUTHORITIES.

   a. Program Secretarial Officers shall:

      (1) Ensure that each DOE and DOE contractor site under their cognizance establishes, implements, and sustains a TEMPEST program in accordance with the requirements of this Order; and

      (2) Implement and coordinate an appropriate management oversight process which ensures awareness and compliance with this Order at cognizant DOE and DOE contractor sites.

   b. Director of Administration and Human Resource Management (AD-1), as the Departmental Designated Senior Official for Information Resources Management (IRM), shall provide the overall leadership and management of DOE's TEMPEST-related activities as required by Department policy and public law.

c. Director of Information Resources Management (AD-20), through the Director of IRM Policy, Plans, and Oversight (AD-24), shall:

(1) Promulgate DOE TEMPEST policy and standards for all classified processing applications and assure compliance;

(2) Represent the Department in all matters concerning TEMPEST;

(3) Plan, program, and budget for Headquarters TEMPEST services and provide budget guidance for field organizations engaged in TEMPEST testing programs or requiring testing;

(4) Provide TEMPEST design and other technical engineering assistance to all Department Elements and their respective contractors and subcontractors;

(5) Serve as the TEMPEST Training Coordinator for the Department;

(6) Conduct an TEMPEST RED/BLACK inspection of DOE and DOE contractor facilities every 2 years, including the Protective Distribution Systems of DOE and DOE contractor facilities;

(7) Appoint the DOE CTTA; and

(8) Review and approve or disapprove:

(a) Proposed unclassified articles and presentations concerning TEMPEST;

(b) Proposals for TEMPEST testing capabilities;

(c) TEMPEST and RED/BLACK certification for shielded enclosures, fully compliant TEMPEST-approved equipment, and sensitive compartmented or special category information facilities;

(d) TEMPEST expenditures over $50,000; and

(e) TEMPEST plans.

d. Director, Naval Nuclear Propulsion Program (NE-60), shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by 42 U.S.C. 7158, note) and to ensure consistency throughout the joint NAVY/DOE organization of NE-1, implement all policy and practices pertaining to this DOE Order for activities under the Director's cognizance.

e. The DOE CTTA is a properly trained and experienced person who serves as the principal TEMPEST technical advisor to the Department, its operating elements, and contractors, and is thoroughly familiar with technical TEMPEST countermeasures, their cost and benefits; and is knowledgeable of threat and vulnerability analysis. The DOE CTTA shall, through AD-24, ensure that TEMPEST countermeasures incorporated at all facilities, and in equipment/system development are consistent with policy. Specifically, the DOE CTTA shall review for approval, and or design:

(1) Any TEMPEST countermeasure that involves radio frequency shielded enclosures and/or fully compliant TEMPEST-certified equipment;

(2) Any TEMPEST expenditures over $50,000, including contractors and subcontractors as specified in paragraph 6d;

(3) Any field element implementation of TEMPEST that does not comply with minimum national security standards as issued under authority of NSD-42. Waivers of DOE requirements must be submitted for review; and

(4) TEMPEST countermeasures for facilities that process special intelligence information.

f. The Administrator, Energy Information Administration, shall appoint a TEMPEST Coordinator for its Headquarters activities.

g. Managers of DOE Field Offices, Managers/Directors of Area Sites, Managers of DOE Contractor Offices, and Director of Information Technology Services and Operations (AD-25) shall:

(1) Have TEMPEST countermeasure authority for information systems operated within their jurisdiction provided:

(a) Minimum national policy issued under authority of NSP-42 is met;

(b) TEMPEST related expenditures are not over $50,000;

(c) Radio Frequency Interference (RFI) shielded enclosure or architectural shielding is not required;

(d) Fully compliant TEMPEST equipment is not required; and

(e) The system or facility does not process special intelligence information.

(2) Refer to the DOE CTTA situations involving expenditures costing over $50,000, use of RFI shielded enclosures and/or architectural shielding, use of fully compliant TEMPEST equipment, or the system or facility processes special intelligence information;

(3) Appoint, in writing, or direct the appointment of a technical or experienced TEMPEST Coordinator of each major DOE or contractor facility under their jurisdiction. The IT Security Division (AD-243) shall be provided a copy of each letter of appointment;

(4) Prepare or direct the preparation of a TEMPEST plan in compliance with stated policy for each DOE and contract facility under their jurisdiction. A certification may be substituted for the plan at facilities which have been evaluated in accordance with this policy as having no TEMPEST countermeasure requirement;

(5) Provide TEMPEST Coordinators with adequate policy guidance and training to enable them to implement the site's TEMPEST program;

(6) Ensure compliance with TEMPEST plans;

(7) Take corrective action recommended by AD-243 to ensure the TEMPEST integrity of the telecommunications or ADP facilities that process classified information;

(8) Comply with all emission security requirements promulgated pursuant to this policy and perform surveys as directed by AD-243;

(9) Maintain a TEMPEST file for each facility;

(10) Include TEMPEST considerations in classified telecommunications development, implementation, operation, and maintenance activities;

(11) Conduct risk analyses of their facilities to determine cost-effective and essential TEMPEST safeguards;

(12) Schedule and conduct annual inspections and compliance reviews at cognizant sites to assess the adequacy of the TEMPEST program, the TEMPEST plan, and the sustained effectiveness of TEMPEST program procedures and to make recommendations for improvement, as appropriate;

(13) Ensure that procedures are implemented for reporting significant incidents or unauthorized interception immediately following detection of the incident to Director, AD-24, and hat significant incident information received from Headquarters is disseminated to appropriate offices and personnel;

(14) Ensure that information related to the TEMPEST program (e.g., information describing specific vulnerabilities or protection features) is provided protection commensurate with the sensitivity of that information when it is collected, stored, distributed, or transmitted;

(15) Ensure that, through the contracting officer, all appropriate contractors are required to comply with the provisions of this Order;

(16) Coordinate requirements of this Order, and related TEMPEST matters, with organizations or individuals having responsibilities for telecommunications security;

(17) Submit to AD-243 for review and approval:

(a) Any proposed unclassified articles and presentations concerning TEMPEST, at least 90 days prior to proposed publication or use;

(b) Proposals for the establishment of a TEMPEST testing capability;

(c) TEMPEST plan; and

(d) Waivers; and

(18) Establish the schedule for zone testing (or retesting).

h. TEMPEST Coordinators shall:

(1) Report directly to the Head of the Field Element, or his designee, except that contractor TEMPEST Coordinators may have to report via a contract monitor;

(2) Serve as the point of contact for TEMPEST matters in their areas of responsibility;

(3) Ensure that the facilities under their jurisdiction are in compliance with TEMPEST guidelines promulgated by AD-24;

(4) Maintain a TEMPEST library of technical publications that is appropriate for their level of responsibility and a file of TEMPEST-related correspondence;

(5) Ensure that scheduling of TEMPEST testing at their facilities is coordinated with AD-243 and the Head of the Field Element, where appropriate;

(6) Ensure that necessary TEMPEST standards are included in the construction of telecommunications and ADP facilities;

(7) Collaborate with procurement personnel so that TEMPEST is considered in the procurement of new equipment, where required;

(8) Collaborate with personnel in various security programs so that applicable TEMPEST policy, standards, and objectives are included in security education programs;

(9) Conduct internal appraisals/reviews to ensure compliance with TEMPEST plans; and

(10) Ensure that recommendations resulting from TEMPEST RED/BLACK inspections are implemented.

8. GENERAL.

a. Each DOE and contractor location which processes classified information shall be evaluated according to national TEMPEST standards, based on this policy.

b. Where zone testing is required, testing shall be conducted at least once every 3 years, if deemed necessary by the cognizant manager, or whenever a significant modification of equipment or threat at the facility occurs.

c. Follow-on testing shall be performed based on the results of zone testing.

d. The basis for all TEMPEST countermeasures shall be a function of threat and vulnerability. All waivers of DOE TEMPEST criteria must be documented.

e. TEMPEST information must be classified in accordance with minimum national requirements. TEMPEST information, even though properly marked "unclassified," cannot be released without prior DOE CTTA approval.

BY ORDER OF THE SECRETARY OF ENERGY:

DONALD W. PEARMAN, JR.
Acting Director
Administration and Human
Resource Management