

9-7-93

TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS

3-4-94

SUBJECT: TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS

1. PURPOSE. To establish policy and provide guidance concerning protected distribution systems used to transmit classified information.
2. CANCELLATION. Department of Energy 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 5-18-92.
3. SCOPE. Except for the exclusions in paragraph 5, the provisions of this Order apply to all Departmental Elements, to include Office of Civilian Radioactive Waste Management personnel and activities not directly associated with Nuclear Regulatory Commission licensed facilities, and thus not covered by the Nuclear Regulatory Commission directives, utilizing protected distribution systems to transmit classified information.
4. APPLICATION TO CONTRACTS. Except for the exclusion in paragraph 5, this Order includes requirements that are to be applied to the universe of contractors who use telecommunications equipment, systems, or facilities to process classified information and are awarded a procurement contract or subcontract.

These contracts shall be required to comply with the responsibilities detailed in paragraph 9g.

5. EXCLUSIONS. The provisions of this Order do not apply to the National Security Agency-approved intrusion detection optical communications system for clear text transmission of classified information. Office of Civilian Radioactive Waste Management personnel and activities directly associated with Nuclear Regulatory Commission licensed facilities covered by Nuclear Regulatory Commission directives are exempt from the requirements of this Order.
6. REFERENCES AND DEFINITIONS. See Attachment 1.
7. POLICY. It is Departmental policy to use the protected distribution system only when the system is designed, engineered, installed, operated and maintained in a manner that ensures emission security (TEMPEST), technical, and physical protection against access by unauthorized personnel.

A protected distribution system is one of three ways in which classified information can be securely transmitted. Use of cryptographic equipment is preferred; intrusion detection optical communications systems is also approved. A protected distribution system is no longer required inside a secure communications center when transmission is from the cryptographic equipment to a terminal. This is a "distributive network," and normal wireline RED/BLACK criteria would apply.

8. ASSISTANCE. Questions concerning this Order should be directed to the Office of IRM Policy, Plans, and Oversight, IT Security Division.
9. RESPONSIBILITIES AND AUTHORITIES.
 - a. Assistant Secretary, Human Resources and Administration, as the Departmental Designated Senior Official for Information Resources Management, shall provide the overall leadership and management of activities related to the protected distribution systems as required by Department policy.
 - b. Director of Information Resources Management, through the Director of IRM Policy, Plans, and Oversight, shall:
 - (1) Develop and coordinate the implementation of Departmental policies, procedures, and guidelines related to the requirements of this Order;
 - (2) Serve as the Departmental point of contact on protected distribution systems and related matters;
 - (3) Coordinate the review and dissemination of information concerning protected distribution systems policy, requirements, and reporting;
 - (4) Establish TEMPEST protected distribution systems requirements for all Department of Energy elements and contractor facilities;
 - (5) Review, concur, or approve, all waivers and exceptions to protected distribution system criteria specified in the Department of Energy "Protected Distribution Systems Procedural Guide;"
 - (6) Provide planning and engineering assistance when requested;
 - (7) Conduct management reviews every 3 years of the Headquarters Elements, operations offices, Rocky Flats Office, and the Office of Information Technology Services and Operations to assess the sustained effectiveness of the management oversight of the protected distribution systems programs established by Department of Energy elements and contractors under their cognizance and make recommendations for improvement, if appropriate; and
 - (8) Develop protected distribution system criteria consistent with the physical and technical security requirements outlined in Department of Energy 6430.1A, GENERAL DESIGN CRITERIA.
 - (9) Coordinate with the Director, Intelligence and National Security, physical and technical security waivers and exceptions of a protected distribution system.
 - c. Director, Office of Intelligence and National Security, shall:
 - (1) Approve the transmission of Top Secret information;
 - (2) Establish physical and technical security requirements for all protected distribution systems used by Department of Energy

elements and contractors.

- (3) Provide an evaluation of all waivers and exceptions from physical and technical security criteria of a protected distribution system to the Office of IRM Policy, Plans, and Oversight.
- d. Senior Intelligence Officer shall, in coordination with the Office of IRM Policy, Plans, and Oversight, approve protected distribution systems used for the transmission or reception of sensitive compartmented information.
 - e. Director of Naval Nuclear Propulsion Program shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by 42 United States Code 7158, note) and to ensure consistency throughout the joint Navy/Department of Energy organization of the Office of Assistant Secretary for Naval Reactors implement and oversee all policy and practices pertaining to this Order for activities under the Director's cognizance.
 - f. Managers of Department of Energy Operations Offices and Rocky Flats Office, and Director, Office of Information Technology Services and Operations, shall:
 - (1) Ensure that each Department of Energy element and contractor under their cognizance establishes, implements, and sustains a protected distribution systems program in accordance with the requirements of this Order;
 - (2) Establish a management oversight process to ensure that Department of Energy elements and contractors under their cognizance are aware of and comply with this Order;
 - (3) Ensure that protected distribution systems program compliance reviews are conducted every 2 years of Department of Energy elements and contractors under their cognizance to assess the sustained effectiveness of protected distribution systems program elements and procedures;

- (4) Designate in writing a Department of Energy employee who is knowledgeable in protected distribution systems programmatic and technical requirements to be the focal point for coordinating protected distribution systems program activities between their organizations and Department of Energy elements and contractors under their cognizance, and the Office of IRM Policy, Plans, and Oversight;
- (5) Ensure each Department of Energy element and contractor under their cognizance develop and implement procedures for identifying incidents involving unauthorized intrusions and reporting them to the Director, Office of IRM Policy, Plans, and Oversight;
- (6) Coordinate requirements of this Order, and related protected distribution systems matters, with organizations/individuals having responsibility for protected distribution systems security;
- (7) Review and approve protected distribution systems requirements and implementation plans; inspect and approve the protected distribution systems to transmit classified information;
- (8) Handle deviations of protected distribution system criteria as identified in the Department of Energy "Protected Distribution Systems Procedural Guide" as follows:
 - (a) review, approve, document, and submit to the Office of IRM Policy, Plans, and Oversight for information all variances;
 - (b) review, approve, and submit for concurrence all waivers to the Office of IRM Policy, Plans, and Oversight;
 - (c) review and submit all exceptions to the Office of IRM Policy, Plans, and Oversight;
 - (d) waivers which create potential or real vulnerabilities and exceptions will normally not be concurred or approved without substantial justification and only in extenuating circumstances.
- (9) Review all protected distribution systems and protected distribution systems proposals for all cognizant Department of Energy elements and contractors to determine applicability of cryptologic technology or secure fiber based on the Office of IRM Policy, Plans, and Oversight guidance; certify that new protected distribution systems or substantial changes to existing protected distribution systems is less costly over the long term than other information security systems or technology, prior to protected distribution systems acquisition;

- (10) Obtain approval of the Office of Intelligence and National Security to transmit or to receive Top Secret information via a protected distribution system and approval of the Office of Intelligence and National Security when sensitive compartmented information is involved;
 - (11) Ensure that all applicable protected distribution systems security requirements for each cognizant site are included in the design, development, implementation, operation, and maintenance of protected distribution systems, as specified by the Department of Energy "Protected Distribution Systems Procedural Guide;" and
 - (12) Ensure that security inspections of protected distribution systems are conducted at cognizant sites.
- g. Managers and Directors of Department of Energy elements, and contractors, shall:
- (1) Ensure that formal approval is received from the cognizant approval authority before operating a protected distribution system, and that each protected distribution system is installed, operated, and maintained in accordance with Departmental requirements;
 - (2) Develop plans for new systems or changes to existing systems in accordance with Departmental requirements;
 - (3) Designate in writing an individual knowledgeable in protected distribution systems operation and installation practices to coordinate activities of this Order;
 - (4) Ensure that Top Secret information and/or sensitive compartmented information is not processed within their protected distribution systems unless written approval has been received;
 - (5) Review protected distribution systems applications and proposed new systems for applicability of secure fiber or cryptographic techniques, and provide comments to the operations office manager;
 - (6) Schedule and conduct internal protected distribution systems reviews every 2 years to assess the sustained effectiveness of protected distribution systems program elements and procedures, and to make recommendations for improvement, as appropriate;
 - (7) Maintain records relative to all protected distribution systems events or incidents; e.g., inspections, results of patrols, alarm events, employee reports, and line route inspections. Records must be available for review during TEMPEST RED/BLACK inspections conducted by the Office of IRM Policy, Plans, and Oversight;

- (8) Develop and implement procedures for identifying incidents involving unauthorized intrusions and reporting them to the cognizant operations office manager or to the Office of IRM Policy, Plans, and Oversight, as appropriate; and
- (9) Submit all requests for deviation from protected distribution system criteria to the appropriate approving authority.

10. GENERAL.

- a. A protected distribution system provides a means for the transmission of unencrypted classified information when economic, technical, and operational factors make that system more suitable than a cryptographic or intrusion detection optical communications system. This is accomplished by the application of TEMPEST and physical security measures to the system. The extent of the measures required shall be dependent upon the existing integrity of the system, the physical security aspects of the area to be traversed, and the classification level of the information to be protected.
- b. A protected distribution system may traverse controlled or uncontrolled access areas or may be installed wholly within an area accessed by cleared personnel with different levels of security clearances. Installation criteria for each system will vary according to the security clearances of unescorted personnel, classification of information being handled, and access controls exercised over these areas. Specific installation criteria can be found in the Department of Energy "Protected Distribution Systems Procedural Guide" and the Department of Energy "RED/BLACK Design/Installation Guide." Specific physical security measures shall be determined by the Departmental Security Office having cognizance over the facility.
- c. Cost and operational impact of maintaining the security of the system must be assessed prior to acquisition and installation, as such cost can easily exceed the installation cost of other systems.
- d. A protected distribution system may only be used after the appropriate authority has approved the system and certified that it is less costly over the long term than other information security systems, it can provide continuing protection, and maintenance and inspection records will be maintained.

11. PLANNING CONSIDERATIONS. Extreme caution shall be observed in planning a system in order to reduce or eliminate security hazards consistent with the judicious use of funds. It is essential that security officials work closely with communications officials to obtain a cost-effective system that affords adequate security protection. Those factors to be considered include:
- a. Evaluation of existing facilities and the security clearance of personnel assigned to a totally secured area, with the objective of selecting the most cost-effective option of either applying basic or modified RED and BLACK techniques; or evaluating whether the security clearance level required by personnel assigned to the area is consistent with the classification level of the material processed within the secured area.
 - b. Comparison of costs and availability of approved encryption devices versus enhanced physical security; i.e., using guards, closed-circuit television, underground cable, or other measures for traversing nonsecure areas as provided for in protected distribution systems.
 - c. Multiplexing of signals on existing secure systems.
 - d. The sharing of fiber optics in conduit or duct with any other wiring (e.g., underground telephone wiring), provided that physical access is limited to cleared or escorted personnel and the old telephone conduit or duct is buried in accordance with the Department of Energy "Protected Distribution Systems Procedural Guide."

BY ORDER OF THE SECRETARY OF ENERGY

REFERENCES

1. Department of Energy 5300.1C, TELECOMMUNICATIONS, of 6-12-92, which establishes policy and general guidance for Department of Energy telecommunications services.
2. Department of Energy 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST), of 5-18-92, which establishes the Departmental program for TEMPEST, and implements the provisions of the national policy that are applicable to TEMPEST.
3. Department of Energy 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 2-3-88, which establishes the Departmental Technical Surveillance Countermeasures Program.
4. Department of Energy 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, of 9-15-92, which establishes uniform requirements, policies, and responsibilities for the development and implementation of a Department of Energy program to ensure the security of information stored in classified automated data processing systems.
5. Classification Guide, CG-SS-2, "Classification Guide for Safeguards and Security Information," of 7-90, which provides guidance for classification of communications security and TEMPEST information.
6. National Communications Security Instruction 4009, "Protected Distribution Systems" (Confidential, title Unclassified), of 12-30-81, National Security Agency.
7. Department of Energy, "RED/BLACK Design/Installation Guide" (Confidential, title unclassified), of 04-1-91, which provides technical TEMPEST RED/BLACK criteria for Department of Energy elements and contractors facilities.
8. Department of Energy, "Protected Distribution Systems Procedural Guide" (Confidential, title Unclassified), of 09-25-86, which provides detailed instructions and procedures for implementing the policies of this Order.
9. Department of Energy 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89, which provides general design criteria for Departmental facilities.
10. Department of Energy 5300.3B, OCCURANCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 2-22-93.

DEFINITIONS

1. COMMUNICATIONS SECURITY. Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, TEMPEST, and physical security of communication security material.
2. EMISSION SECURITY. Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems, and telecommunications systems.
3. PROTECTED DISTRIBUTION SYSTEM. A wireline or a fiber optic system that includes adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information.
4. RED/BLACK. A term used to describe separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain language information in electric signal form (RED) differ from those which handle unclassified information (BLACK). RED and BLACK terminology is used to denote specific criteria relating to, and to differentiate between, such circuits, components, equipment, and systems and the areas in which they are contained.
5. SENSITIVE COMPARTMENTED INFORMATION. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director, Central Intelligence Agency, pursuant to the special access provisions of Executive Order 12356.
6. TECHNICAL SURVEILLANCE COUNTERMEASURES. Those measures taken to prevent, detect, and neutralize efforts to acquire classified information by technical surveillance.
7. TEMPEST. A short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems.
8. VARIANCE. A variance is an approved condition that technically varies from the Department of Energy protected distribution system criteria, but affords equivalent levels of protection.
9. WAIVER. A waiver is an approved nonstandard condition that deviates from the Department of Energy protected distribution system criteria which, if equivalent protection cannot be satisfied, would create a potential or real vulnerability. The waiver will not exceed 2 years.
10. EXCEPTION. An exception is an approved deviation from the Department of Energy protected distribution system criteria that creates a vulnerability because corrections to the nonstandard conditions are not feasible or are inadequate.