U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5300.3D

8-3-93

SUBJECT: TELECOMMUNICATIONS: COMMUNICATIONS SECURITY

1. **PURPOSE.** To establish policy, responsibilities, and guidance concerning the communications security and automated information systems security aspects of the telecommunications services of the Department of Energy.

2. **CANCELLATION.** DOE 5300.3C, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, 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 Nuclear Regulatory Commission directives.

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 awarded a procurement contract or subcontract.

5. **EXCLUSIONS.** 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. **APPLICABILITY.**

   a. This Order prescribes communications security responsibilities and authorities. It also provides policy on the planning, engineering, installation, operation, maintenance, and control of communications security material. Such material encompasses both Government-furnished equipment and commercial devices that employ the data encryption standard. This Order applies to all forms of telecommunications, including narrative, voice, data, video, imaging, and facsimile information exchange and the major components employed to protect information, including:

      (1) Government cryptographic equipment, software, and associated keying material;

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Information Resources Management

(2) General communications security instructional documents, operating instructions, and maintenance materials;

(3) Crypto-ancillary hardware or software designed specifically to facilitate operation of crypto-equipment; and

(4) Commercial devices employing the data encryption standard when authorized by the Department.

b. All communications security information is considered sensitive because of the need to safeguard United States cryptographic principles, methods, and material against exploitation and to protect the classified information encrypted in the United States cryptosystems.

7. REFERENCES AND DEFINITIONS. See Attachment 1.

8. POLICY.

a. The National Security Telecommunications and Information Systems Security Policy contains the following:

(1) United States Government national security systems shall be secured by such means as are necessary to prevent compromise, denial, or exploitation; Federal agencies shall require that national security systems operated and maintained by United States Government contractors likewise be secured.

(2) Systems handling other sensitive, but unclassified, Government or Government-derived Information, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and associated potential damage to the national security.

b. It is the policy of the Department of Energy to:

(1) Provide a reliable and responsive communications security capability for Department of Energy telecommunications in accordance with the national policy. All classified information transmitted via Departmental telecommunications shall be secured by using National Security Agency–approved cryptographic equipment or protected distribution systems. Unclassified national

security-related information of value to an adversary transmitted by and between Government elements and contractors will be given communications protection commensurate with the associated risk of exploitation.

(2) Operate a central office of record and a communications security material control system to direct, manage, and control the acquisition, distribution, accountability, and disposition of communications security materials within the Department.

9. ASSISTANCE. Questions concerning this Order should be directed to the Office of IRM Policy, Plans, and Oversight, IT Security Division.

10. RESPONSIBILITIES AND AUTHORITIES.

a. Heads of Departmental Elements shall:

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

(2) Appoint in writing communications security control officers, custodians, and their alternates. Instructions for preparation of the written appointment letters are contained in the 'Department of Energy Communications Security Procedural Guide." Appointment letters are required for all crypto-personnel.

(3) Through technical requirements personnel and procurement request initiators, specify the requirements of this Order in statements of work and specifications for use in solicitations and contracts.

(4) Ensure that documents prepared under this Order are reviewed for classified or controlled information.

b. Assistant Secretary, Human Resources and Administration, as the Departmental Designated Senior Official for Information Resources Management, shall provide the overall leadership and management of the Department of Energy's communications security-related activities as required by Department policy and public law.

c. Director of Information Resources Management, through the Director of IRM Policy, Plans, and Oversight, shall:

(1) Represent the Department of Energy on the National Security Telecommunications and Information Systems Security Committee;

(2) Establish policy and provide direction, administration, and coordination of the communications security program throughout the Department. This includes transmission security, emission security, cryptosecurity, and associated control, audit, and training activities;

(3) Appoint the communications security officer (communications);

(4) Evaluate notifications of security irregularities involving communications security to determine their effects on the security integrity of Departmental telecommunications systems and notify holders of communications security material of required corrective action. Coordinate with representatives of the Director, Office of Intelligence and National Security, and forward appropriate reports to the National Security Agency.

(5) Serve as the central office of record for communications security accounting. Approve the appointment and administer the activities of the Department communications security control officer.

(6) Work with the Director, Office of Intelligence and National Security, to obtain authorization to release communications security equipment and material to contractors for their operational use.

(7) Review the effectiveness and efficiency of Departmental secure communications operations and recommend or initiate improvements where necessary.

(8) Approve Departmental use of equipment employing the data encryption standard.

(9) Review and approve all proposals for use of embedded cryptographic technology for classified operating information technology systems and provide technical

assistance in product selection, design, integration, and testing.

(10) Specifically approve purchase of cryptographic devices not compatible with the electronic key management system.

d. Director, Office of Information Technology Services and Operations, shall provide for the proper installation and maintenance of communications security equipment for the Department and its contractors.

e. Director, Office of Intelligence and National Security, shall:

(1) Direct, administer, and coordinate all policy aspects of clasified *or* controlled (e.g., Unclassified Controlled Nuclear Information) information (except as delegated to other reorganizations in this Order) .

(2) Establish policies, procedures, and standards for the physical security of communications security material and communications security facilities.

(3) Establish policies, procedures, and standards for personnel security.

f. Communications Security Officer (Communicational, shall:

(1) Advise the Department on communications security.

(2) Serve as the Headquarters point of contact with field organizations and with other Federal agencies on Departmental communications security activities.

(3) Review and decide upon requests and proposals for communications security services. Provide staff advice and assistance regarding the design, engineering, installation, operation, and maintenance of communications security facilities.

g. Departmental Communications Security Control Officer, shall:

(1) Maintain the central office of record and the communications security material control system.

(2) Serve as the Department Top Secret communications security control officer who receives, distributes, and accounts for Top Secret communications security material.

h. Other Communications Security Personnel. The 'Department of Energy Communications Security Procedural Guide" provides detailed descriptions with respect to the following functions and their responsibilities assigned to the:

(1) Communications security control officer;

(2) Communications security custodian;

(3) Crypto-operator; and

(4) Communications security training instructor.

i. *Director,* 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 Deputy Assistant Secretary for Naval Reactors, implement and oversee all policy and practices pertaining to this Order *for* activities under the Director's cognizance.

11. PLANNING OF CRYPTO-FACILITIES. The guidelines and procedures to be followed in the planning of crypto-facilities are described in the "Department of Energy Communications Security Procedural Guide," DOE 6430.1A, GENERAL DESIGN CRITERIA, and Department of Energy physical security orders.

12. ENGINEERING AND INSTALLATION OF CRYPTO-FACILITIES.

a. Crypto-center design, engineering, and installation shall be carried out as directed by the 'Department of Energy Communications Security Procedural Guide," DOE 6430.1A, and Department of Energy physical security orders.

b. Equipment shall not be modified unless directed by the National Security Agency, or by the Office of IRM Policy, Plans, and Oversight (under delegation of authority by the National Security Agency). Each modification directive will contain a deadline for accomplishment. Unmodified equipment is prohibited from operational use after the deadline date.

13. ACQUISITION OF COMMUNICATIONS SECURITY MATERIAL.

a. All requests for communications security material shall be handled between the requesting organization and the Departmental Communications Security control officer.

b. All communications security material, with the exception of Secure Telephone Unit (STU-III), keying material, shall be controlled through the Department of Energy communications security material control system. STU-III keying material shall be controlled through the National Security Agency Key Management System. Guidelines, limitations, and procedures for acquisition of material and certain crypto-related equipment supplies are contained in the 'Department of Energy Communications Security Procedural Guide." The Instructions apply to all Departmental Elements and shall be applied to contractors, except where other arrangements are specifically authorized by the Office of IRM Policy, Plans, and Oversight.

c. Requests for information, installation, or relocation of communications security equipment shall be submitted to the Office of Information Technology and Services Operations. Since such requests may contain classified information, requesters should consult approved classification guidance to determine whether the request is classified or handled as "Official Use Only."

d. Purchase orders for communications security equipment and ancillaries shall be submitted directly to the National Security Agency or the commercial vendor with a copy to the Office of IRM Policy, Plans, and Oversight. The requesting organization must ascertain that the purchase order has been accepted by the National Security Agency or the commercial vendor. The Office of IRM Policy, Plans, and Oversight will assist in this endeavor.

14. DISTRIBUTION OF COMMUNICATIONS SECURITY MATERIAL. Cryptomarked material and accountable crypto-related material shall be distributed through the Department communications security distribution channel in accordance with procedures described in the "Department of Energy Communications Security Procedural Guide."

15. ACCOUNTING FOR COMMUNICATIONS SECURITY MATERIAL. All accountable material shall be entered into the communications security material control system at the time of origin (except for STU-III keying material) unless specifically exempted by the Director, National Security Agency, or the Office of IRM Policy, Plans, and Oversight. It is the responsibility of each individual charged with the custody of such material to know at all times the exact location of each item entrusted to his or her care and the general purpose for which it is being used. Communications security material of all classifications shall be accounted for by means of the communications security accounting system and

shall be exempted from other accounting systems, including the Top Secret document control system.

16. INVENTORY REQUIREMENTS FOR COMMUNICATIONS SECURITY MATERIAL. Communications security material must be inventoried periodically as required by National Communications Security Instruction 4005, 'Safeguarding and Control of Communications Security Material," of 10-12-79. Keying material will be inventoried on a semiannual basis. Communications security equipment, components, and communications security publications will be Inventoried at periodic intervals not to exceed 1 year. All inventories will be conducted jointly by any individual appointed to the account and an appropriately cleared witness. Specific instructions for completion of these inventories are included in the "Department of Energy Communications Security Procedural Guide."

17. COMMUNICATIONS SECURITY ACCOUNT OPERATIONS. General guidelines and standard procedures for operation of Departmental and contractor communications security accounts are set forth in the National Security Agency documents and related Departmental supplements. Communications security account operations encompass standard operating procedures, equipment operation, circuit operation, message handling, communications security material handling, records, destruction reports, crypto-operations under abnormal conditions, and crypto-operations under natural emergency conditions.

18. TRAINING REQUIREMENTS. Training requirements for communications security personnel are included in the 'Department of Energy Communications Security Procedural Guide."

19. OTHER COMMUNICATIONS SECURITY OPERATIONS.

a. Other communications security operations include crypto-guard service, interdepartment crypto-operations, crypto-operations outside crypto-centers, crypto-operations outside the continental United States, and noncryptographic secure communications. Details are provided in the "Department of Energy Communications Security Procedural Guide."

b. Operation of Departmental crypto-systems outside the continental United States is subject to prior coordination with the Office of IRM Policy, Plans, and Oversight and the approval of the Office of Intelligence and National Security. Information regarding proposed operations should be submitted in writing to these two responsible organizations.

20. MAINTENANCE OF COMMUNICATIONS SECURITY EQUIPMENT. Routine adjustment and cleaning of certain types of communications security equipment are performed by Department and contractor crypto-operators in accordance with the applicable National Security Agency operating instructions manuals. Installation, maintenance, and repair of communications security equipment will be performed by qualified maintenance personnel of the General Services Administration.

21. COMMUNICATIONS SECURITY AUDITS AND SURVEYS.

a. Audits and surveys of each Department and contractor communications security account and cryptofacility shall be conducted by the Office of IRM Policy, Plans, and Oversight biennially or more often if required. These audits and surveys shall pertain to the conduct of cryptologic activities, including crypto-security, transmission security, emission security, and accounting of communications security equipment, material, and operation of communications security accounts. If possible, the cognizant control officer shall accompany the representatives conducting the survey.

b. Department and contractor communications security control officers may conduct local audits and surveys at any time for the purpose of reviewing the adequacy of their facilities and procedures.

22. DATA ENCRYPTION STANDARD.

a. The data encryption standard specifies that an algorithm is to be implemented in electronic devices and used for the cryptographic protection of narrative, voice, data, video, imaging, and facsimile information. The standard is used within the Department as a technical safeguard to protect sensitive data. The data encryption standard will be used when the Head of a Departmental Element, or authorized representative, deems that telecommunications protection is required for Government-derived sensitive data that are not classified according to the Atomic Energy Act of 1954, as amended, or Executive Order 12356.

b. Departmental Elements that have National Security Agency–approved communications security equipment to secure classified data may use this equipment, in lieu of the data encryption standard, for protecting sensitive data.

c. Organizations and contractors that require the application of commercial devices employing the data encryption standard

shall submit their requirements to the Office of IRM policy, Plans, and Oversight for review, coordination, and approval.

d. Keying material to support data encryption standard may be obtained from the National Security Agency through the central office of record or may be created locally. Federal Information Processing Standard Publication 171, “Key Management Using American National Standards Institute X9.17," of 04-27-92, must be adhered to when creating data encryption standard keys. Development of data encryption standard keys locally must be coordinated with the central office of record.

e. Keying material shall be controlled locally.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary For Human Resources and Administration

REFERENCES

1. DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, of 5-18-92, which establishes policies and procedures for developing, implementing, and administering a program for safeguarding the Department of Energy computer systems and, in particular, Department of Energy-sensitive unclassified information.

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

3. DOE 300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST), of 5-18-92, which establishes the Departmental program for emission security and implements the provisions of the national policy which are applicable to emission security.

4. DOE 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. DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-6-89, which provides general design criteria for use in the acquisition of the Department's facilities and to establish responsibilities and authorities for the development and maintenance of these criteria.

6. 'Department of Energy Communications Security Procedural Guide," of 7-91, (Revision 4 of 1-93), which provides detailed instructions and procedures for implementing the communications security policies of this Order, and is issued to those elements involved in the communications security program.

7. CG-SS-2,"Classification Guide for Safeguards and Security Information" (Including Confidential Annex), of 7-90, which provides guidance for classification of communications security and emission security.

8. Executive Order 12344, "Naval Nuclear Propulsion Program," of 2-1-82, which assigns responsibilities and authorities for the Nuclear Propulsion Program.

9. Executive Order 12356, "National Security Information," of 4-2-82, which provides requirements for safeguarding National Security Information.

10. Federal Information Processing Standards Publication 46-1, "Data Encryption Standard," of 4–77, and reaffirmed 6-77, which provides an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of certain United States Government information.

11. National Security Telecommunications and Information Systems Security publications, including: Policies, Directives, Instructions, and Advisory Memorandums. These publications can be made available through the Department of Energy communications security central office of record, IT Security Division.

12. "National Telecommunications and Information Systems Security Policy No. 1," of 6-17-85, entitled "National Policy on Application of Communications Security to National Security-Related Civil and Commercial Space Systems."

13. "National Communications Security Committee-n, National Policy for Protection of Telecommunications Systems Handling Unclassified National Security-Related Information," of 5-3-82, which establishes the United States Government policy for protection of such systems.

DEFINITIONS

1. COMMUNICATIONS SECURITY is 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, emission security, and physical security of communications security material.

2. COMMUNICATIONS SECURITY MATERIAL CONTROL SYSTEM provides administrative control of Department of Energy communications

security material. which, for example, includes equipment, keying variables, publications, and modifications to equipment. This control is in the area of receipt, assignment, accountability, equipment improvements, impact of security violations, and disposition of communications security material.

3. DATA ENCRYPTION STANDARD is a standard algorithm implemented in electronic hardware devices used for cryptographically protecting sensitive unclassified United States Government information. (See Federal Information Processing Standard Publication 46-1.)

4. EMISSION SECURITY (more commonly known as TEMPEST) is the 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.

5. REPORTABLE INSECURITIES are all deviations from rules of communications security (crypto-security, transmission security, emission security, and physical security) or any occurrence which may detrimentally affect the security of communications security information or encrypted communications. (Occurrences that require reports are listed in the National Security Agency communications security publications, the "Department of Energy Communications Security Procedural Guide," and in specific operating instructions and maintenance manuals.)