

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

SAFEGUARDING AND CONTROL OF

DATA ENCRYPTION STANDARD (DES)

EQUIPMENT AND ASSOCIATED

UNCLASSIFIED COMMUNICATIONS SECURITY AIDS

Approved for Release by NSA on 09-25-2024, FOIA Case # 51573

~~FOR OFFICIAL USE ONLY~~

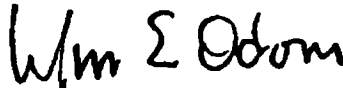
NTAISSNATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY**NATIONAL MANAGER**

16 March 1987

FOREWORD

1. This instruction establishes minimum standards and physical security guidelines for the protection of NSA-approved unclassified commercial and government-developed Data Encryption Standard (DES) equipments and associated keying material which are employed in the protection of sensitive, but unclassified, information, the loss of which could adversely affect the national security interest.
2. This instruction and any excerpts may be given to government contractors, but cannot be given to the general public without the approval of the National Manager, NTAISS.
3. Heads of Federal Departments and Agencies are responsible for distributing this NTISSI to their subordinate elements. Additional copies may be obtained from:

Executive Secretariat
National Telecommunications and Information
Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000



WILLIAM E. ODOM
Lieutenant General, USA

~~FOR OFFICIAL USE ONLY~~

SAFEGUARDING AND CONTROL OF DATA ENCRYPTION
STANDARD (DES) EQUIPMENT AND ASSOCIATED
UNCLASSIFIED COMMUNICATIONS SECURITY AIDS

SECTION

PURPOSE AND SCOPE. I
DEFINITIONS II
RESPONSIBILITIES III
PHYSICAL SECURITY IV
EQUIPMENT MAINTENANCE. V
KEYING. VI
DESTRUCTION. VII
INSECURITIES. VIII

SECTION I - PURPOSE AND SCOPE

1. National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," requires that sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national interest, shall be protected in proportion to the threat of exploitation and the associated potential harm to the national interest. Some commercial equipments using the DES algorithm have been endorsed by the National Security Agency (NSA) to provide this protection. This instruction prescribes minimum controls and procedures for safeguarding this equipment and its associated key and unclassified communications security (COMSEC) aids. Each department and agency may prescribe additional controls and procedures as deemed necessary. This instruction is applicable to all departments and agencies of the government and government contractors.

2. Unclassified DES protection equipment used to protect sensitive, but unclassified, information is available from commercial vendors. Commercial DES equipment must be endorsed by the Director, NSA, prior to its use to protect government information. A list of endorsed DES equipment may be obtained from:

Director
National Security Agency
ATTN:
Fort George G. Meade, MD 20755-6000

(b) (3)-P.L. 86-36

SECTION II - DEFINITIONS

3. Definitions contained in the National COMSEC Glossary (NCSC-9) apply. For the purpose of this instruction, the following terms also apply:

- a. Key Loader. An ancillary device used to transfer, store, or load key into a protection equipment.
- b. Physical Key. A device used to operate a mechanical lock.
- c. Key. A sequence of random binary bits used to initially set up and periodically change the encryption/decryption function in a protection equipment for purposes of the encryption, decryption, or authentication of information.
- d. User COMSEC Account. An administrative entity, identified by an account number, responsible for maintaining custody and control of COMSEC material.
- e. Government Contractor. An individual, corporation, partnership, association, or other entity performing work under a U.S. Government contract, either as a prime contractor, or as a subcontractor.

SECTION III - RESPONSIBILITIES

4. National Security Agency. The National Security Agency is responsible for:

- a. Evaluating and endorsing cryptographic systems and doctrine for the protection of sensitive, but unclassified, government or government-derived information.
- b. Producing or approving the production/reproduction of all keying material used in cryptographic systems for the protection of government information.
- c. Maintaining a record of all active cryptonets and COMSEC accounts under its control.
- d. Assigning an Accounting Legend Code (ALC) for the control of NSA-produced keying material.
- e. Evaluating requests for authorization of equipment maintenance by other than U.S. citizens.
- f. Evaluating reported insecurities when sabotage or espionage is suspected.

g. Providing assistance or guidance to department and agency heads upon request to determine risk of hostile exploitation.

5. Government Department and Agency Heads and Government Contractors. Heads of departments and agencies which use, or contract for the use of, approved DES protection equipment and related unclassified aids are responsible for:

a. Determining which of their unclassified information, intended for transmission, requires protection and the risk of exploitation of that information.

b. Establishing and maintaining a Central Office of Record (COR) to maintain records of all accountable COMSEC material received by, or generated within, the department or agency or its contractors. The COR is responsible for supervision of all subordinate COMSEC accounts. It will forward requests from department or agency subordinate elements or contractors for the establishment of COMSEC accounts for the handling of NSA-produced keying material. COMSEC accounts established to retain classified COMSEC material can be used for unclassified material. When necessary, an unclassified COMSEC account may be established solely to maintain unclassified material. Persons selected to be custodians and alternate custodians of unclassified accounts must be U.S. citizens. They need not possess a government clearance. When requesting the establishment of this type of account, the following information must be forwarded to the Director, NSA, ATTN:

(1) Title and complete address of the organization where the account will be located, and a name and telephone number for the organization's point of contact for further information.

(2) COMSEC material to be included in the account.

(3) A statement that minimum physical security standards prescribed by this NTISSI for safeguarding the keying material can be met.

c. Providing operational guidelines and logistics support direction for the planning, acquisition, operation, and use of commercial or government-produced protection equipment and related aids.

d. Initiating a periodic evaluation of keying material to ensure that it continues to meet the operational and crypto-security needs of the users.

NTISSI No. 3005

e. Designating controlling authorities to direct the operation of cryptonets within their department or agency. When cryptonets involve both government and government contractor, the government department or agency will be responsible for designating the controlling authority. When the cryptonet members are outside of a government-sponsored organization, the government contractor department or agency sponsoring the cryptonet will appoint the controlling authority.

6. Controlling Authority. The controlling authority's function is normally performed by the senior organization within the net. It is the controlling authority's responsibility to direct the operation of cryptonets. This includes:-----

a. Notifying the Director, NSA, ATTN: , when a new cryptonet is established. This is accomplished by ordering initial and subsequent supplies of keying material (in accordance with the provisions of the annex to this instruction). Normal lead-time for requesting new keying material is 90-120 days.

b. Preparing cryptonet operating instructions to include, as a minimum, designation of the cryptonet members; specifying key change time for the cryptonet; establishing procedures for reporting incidents involving jeopardy to the key or faulty keying material; implementing procedures for emergency destruction, supersession, or extension of cryptoperiods; and advising the Director, NSA, ATTN: , of matters affecting keying material requirements.

c. Prescribing the status, including effective date, for each edition of keying material and keeping all members of the cryptonet(s) informed.

d. Conducting evaluations initiated by parent departments or agencies. Periodically reviewing operational requirements to confirm that the cryptonet is still needed, the membership of the cryptonet is current, the COR is notified of changes in net membership, and the quantities and adequacy of keying material, including contingency material, meet the net members' needs. The COR is the office charged with the accountability of all accountable COMSEC material received by the department or agency.

e. Evaluating the impact of reports of physical loss of control over superseded, effective, and future editions of keying material.

7. COMSEC Custodian and Alternate COMSEC Custodian. It is the custodian and alternate custodian's responsibility to manage a COMSEC account, to include:

- a. Receipt, storage, accountability, issuance, and transfer of the keying material.
- b. Enforcing access controls.
- c. Advising users and supervisors of the required safeguarding and control procedures, and authorized destruction procedures for superseded keying material.
- d. Performing an inventory upon change of custodian or at the direction of higher authority. Inventory records should be maintained at the account to provide continuous administrative control of the keying material. Form SF-153 may be used for inventory purposes. Inventory records should be kept for 90 days.
- e. Notifying the COR upon change of custodian or alternate custodian.

SECTION IV - PHYSICAL SECURITY

8. Keying material marked CRYPTO and keyed protection equipment covered by this instruction must be handled in a controlled manner to preclude unauthorized access, theft, loss, and tampering. This includes control of physical keys and use of area access controls. Area access controls should supplement the built-in physical security (mechanical locks) in installed equipment, particularly in areas which are normally unmanned. Keyed DES equipment will be controlled and protected in the most secure manner available to the user. Exposure of key or access to keyed equipment by unauthorized parties puts at risk communications that are being protected.

9. Unkeyed DES equipment will be controlled and protected as highly valued property and should not be released to foreign nationals without prior NSA approval.

10. Access.

a. Success in protecting secure communications is primarily a function of protecting the CRYPTO keying material. Controlling access to keying material marked CRYPTO is the best method to ensure effective protection. For example, communications equipment operators normally should be given access to only the current edition of keying material. Future keying material should be stored where access is strictly limited to the COMSEC custodian and alternate. Rigid enforcement of the need-to-know principle is the best tool available to achieve this objective. CRYPTO is a reminder to use the "need-to-know"

NTISSI No. 3005

principle. Any procedures that deny even momentary unauthorized access are worth implementing.

b. Ordinarily, protection equipment and keying material covered by this instruction are accessible only to U.S. citizens, permanent resident aliens who are U.S. Government civilian employees, and active duty or reserve members of the U.S. Armed Forces whose duties require access. However, local U.S. commanders and civilian equivalents at field locations are authorized to release keyed DES equipments to foreign nationals in direct support of U.S. personnel during critical, local situations. Foreign nationals involved in such situations may not receive or have access to keying material and key loaders, or be advised that the loaned equipment contains DES cryptography. Access to the equipment by foreign nationals must not exceed the duration of the critical operation. When the equipment is returned, it must be inspected and accounted for to ensure that it has not been tampered with. Should foreign nationals use keyed DES equipment, the controlling authority must be notified immediately to ensure proper secure operation of the cryptonet and take other measures as necessary (e.g., notifying other U.S. net members). In addition, DIRNSA must be informed within 48 hours when any DES equipment is loaned to foreign nationals in direct support of U.S. operations.

11. Storage. Keying material marked CRYPTO, keyed equipment, and keyed key loaders must be stored in the most secure manner available to the user (i.e., approved safes, if available, locked file cabinets, key-locked rooms, desks, containers, etc.). Keys must be cleared when the equipment will not be used operationally for a period in excess of 24 hours. Unkeyed equipment and unkeyed key loaders should be stored as highly valued government property.

12. Accounting. NSA-produced keying material is distributed through, and accountable in, the COMSEC Material Control System (CMCS). Keying material distributed through the CMCS is assigned an Accounting Legend Code (ALC). Keying material for use with the DES protection equipments covered by this instruction will be assigned ALC-3. ALC-3 keying material is accountable by register number printed on the keying material to the COR until issued and receipted by a user COMSEC account. After receipt of ALC-3 keying material by the COMSEC account, it will be controlled locally in accordance with the following as a minimum:

a. Tape canisters should be checked upon receipt to ensure that quantities, register numbers, edition, and short titles coincide with those listed on the transfer report form (SF-153), and that each canister begins with tape segment number one. Tape segments must not be removed from canisters until

needed to key equipment. Any discrepancies should be reported within the local accounting system.

b. Keying material shall be issued by the COMSEC account to users on a formal record (log or hand receipt), showing who the keying material was issued to and the date of issue. This record shall be retained by the user COMSEC account for a minimum of 90 days after supersession of the material. A primary purpose of this record is to permit traceability in the event the material is found outside of authorized channels.

13. Distribution.

a. Packaging. Keying material should be double-wrapped and securely sealed. The inner and outer packaging will contain specific addressing information for the COMSEC custodian or individual authorized to receive the material, with no indication as to package contents. Additionally, the inner package will contain the instruction "To Be Opened Only By COMSEC Custodian or Authorized Individual," and the "CRYPTO" marking. Keying material should not be placed in the same package as protection equipment and key loaders.

b. Means of Transportation. Within the U.S., unclassified keying material may be shipped by either authorized department, agency or contractor courier or U.S. Registered Mail. Outside the U.S., it will be transported by either authorized department, agency or contractor courier, U.S. Diplomatic Courier Service, or Armed Forces Courier Service. U.S. Registered Mail may be used overseas provided the material is forwarded to an APO/FPO address. It may not pass through any foreign postal service, nor may commercial courier services be used overseas.

c. Limitations on Shipments. Individual shipments of keying material should be limited in size to reduce the effects of loss or compromise. When practicable, keying material transported by courier should be limited to no more than three editions; or by U.S. Registered Mail, to no more than one edition.

14. Equipment Inspections. Regular inspections, especially at unmanned sites, increase the likelihood of early detection of tampering, thereby limiting adverse effects on system protection. Protection equipment should be inspected prior to installation and use, and periodically thereafter. When control is regained over an equipment which had been lost, the equipment should be examined to verify that it is unchanged in form and function before it is used.

15. Zeroization. When protection equipment and key loaders will not be under the control of authorized personnel (e.g., prior to storage, shipment, maintenance, and disposition), the equipment must be zeroized by clearing the key. Keys must also be cleared when the equipment will not be used operationally for a period in excess of 24 hours.

SECTION V - EQUIPMENT MAINTENANCE

16. DES protection systems and equipments incorporate certain cryptographic security designs and features. Whenever possible, the maintenance of DES equipments should be performed by U.S. Government personnel. However, if this is not possible, DES equipments may be maintained by U.S. citizens or resident aliens of the U.S. who are employed by U.S. contractors. To avoid possible compromise of these security features, users should select only contractors who have the proper maintenance training on the DES equipment. In addition, contractors must have the required test equipment and manufacturer's maintenance documentation necessary to perform maintenance to the manufacturer's specifications. Only replacement parts approved by the manufacturer may be used in the maintenance or repair of the DES equipment. Proposals for DES equipment maintenance by other than U.S. Government personnel, or U.S. citizens or resident aliens employed by U.S. contractors, must be referred to NSA for prior approval on a case-by-case basis.

17. Modifications may affect the protection capability of the equipment and proposed changes (other than those made for cosmetic reasons) and, therefore, must be coordinated with the Director, NSA, ATTN:

(b) (3) - P.L. 86-36

SECTION VI - KEYING

18. NSA-produced keying material for these systems is unclassified, marked CRYPTO, and is assigned TSEC nomenclature, an alphanumeric designator identifying unclassified keying material.

19. Types of Key. The following are the different types of keying material:

- a. Operational - Key intended for on-the-air use for protection of mission-related, operational traffic; i.e., traffic encryption key (TEK) and key encryption key (KEK).
- b. Maintenance - Key intended only for off-the-air, in-shop use.

c. Training - Key intended for on-the-air training with COMSEC equipment.

d. Test - Key intended for on-the-air testing of COMSEC or communications equipment or systems.

e. Contingency - Key held for use on a cryptonet planned for establishment under specific operational conditions or in support of specific contingency plans.

20. Cryptonet Sizes. Using organizations must give careful consideration to decisions on cryptonet size; i.e., the number of subscribers who must communicate on a single key. Cryptonets should be kept as small as operationally feasible. Generally, small cryptonets narrow the exposure of individual editions of keying material, limit the consequences of keying material compromises in terms of vulnerable communications, and lessen the problems associated with resupply.

21. Cryptoperiods. The cryptoperiod for DES key is seven days. Normally, there are five key segments per canister with each edition (canister) superseded on a monthly basis. Shorter cryptoperiods are encouraged, because shorter cryptoperiods minimize the adverse effects of key compromises. The controlling authority may authorize emergency cryptoperiod extensions of an additional week for mobile communications due to operational or logistic considerations. Longer cryptoperiods must be approved on a case-by-case basis by DIRNSA, ATTN: . Implementation dates for DES keying material, keying material short titles, and effective dates are all unclassified.

SECTION VII - DESTRUCTION

(b) (3) - P.L. 86-36

22. In addition to normal supersession, keying material marked CRYPTO may also be subjected to precautionary supersession by the controlling authority when it has been subjected to (or is suspected of) unauthorized exposure. Keying material should be destroyed in the presence of a witness as soon as possible after supersession, but not later than 12 hours. Tape segments must be destroyed in a manner sufficient to preclude any reasonable chance of recovery of the key. Authorized methods are burning, pulverizing, chopping, crosscut shredding, and disintegrating.

SECTION VIII - INSECURITIES

23. Persons who handle keyed protection equipment, key loaders, and keying material must be aware of the adverse effects

NTISSI No. 3005

of tampering and unauthorized access. All cases of actual or suspected tampering, loss, theft, and unauthorized access are considered insecurities and must be reported to the controlling authority for evaluation. Insecurities where sabotage or espionage are suspected must be reported to the Director, NSA, ATTN:

(b) (3) - P.L. 86-36

Encl:

Annex - Procedure for Requesting
Unclassified Keying Material

PROCEDURE FOR REQUESTING UNCLASSIFIED KEYING MATERIAL

1. Requests for unclassified keying material should be forwarded to:

Director
National Security Agency
ATTN:
Fort George G. Meade, MD 20755-6000

2. Requests should include the following information:

- a. Type of equipment: (manufacturer, equipment nomenclature, model number, and USGEID number, when appropriate).
- b. Controlling Authority: (organization name).
- c. Point of contact and telephone number:
- d. Nature of request: (new requirement, change in requirement, or resupply).
- e. Use: (operational, maintenance, training, testing, or contingency).
- f. Type: (printed or punched paper tape).
- g. Cryptoperiod: (one day or seven days).
- h. Number of editions required:
- i. Copy count for each edition: (self-explanatory).
- j. Ship to: (specify number of copies to be sent to each account listed).
- k. Date required: (90 to 120 days lead time required).
- l. Special instructions: (as required).

3. When the cryptonet is initially implemented so that follow-on production begins on time to keep pace with usage, NSA, ATTN: will be notified.

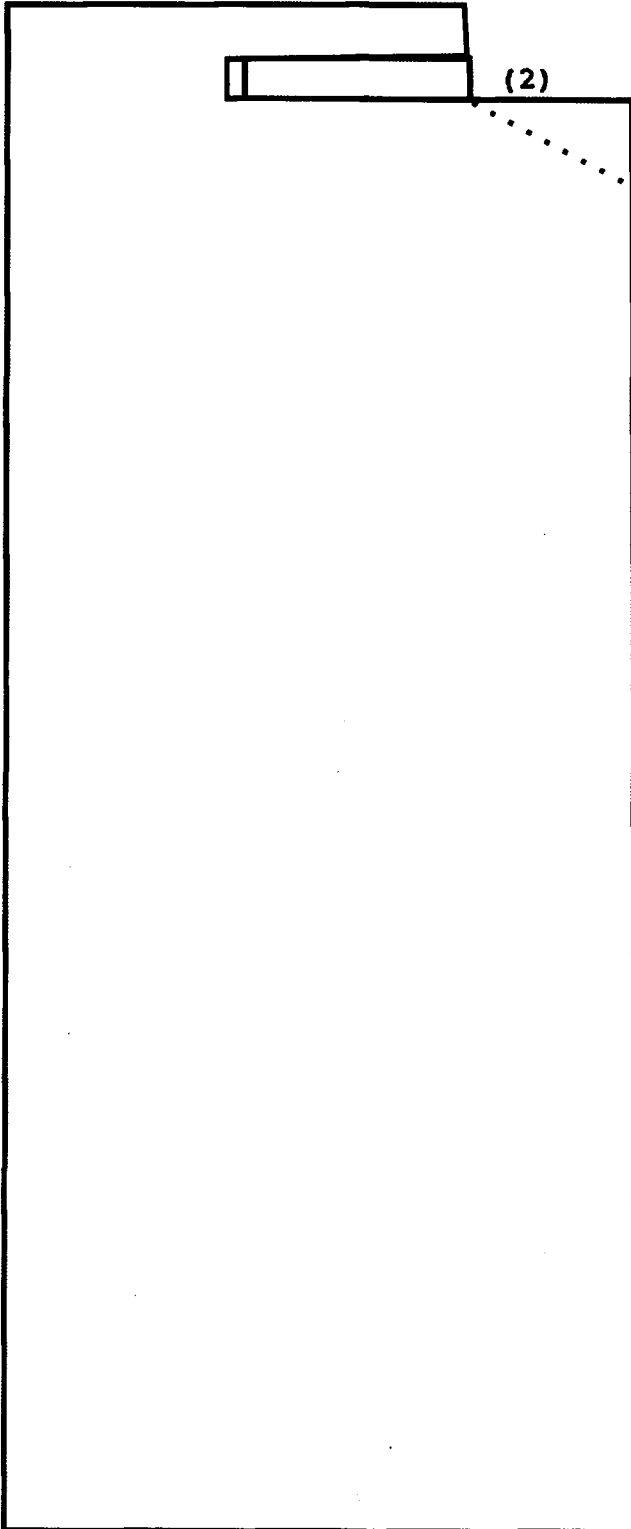
(b) (3) - P.L. 86-36

Annex to
NTISSI No. 3005

~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:

NSA

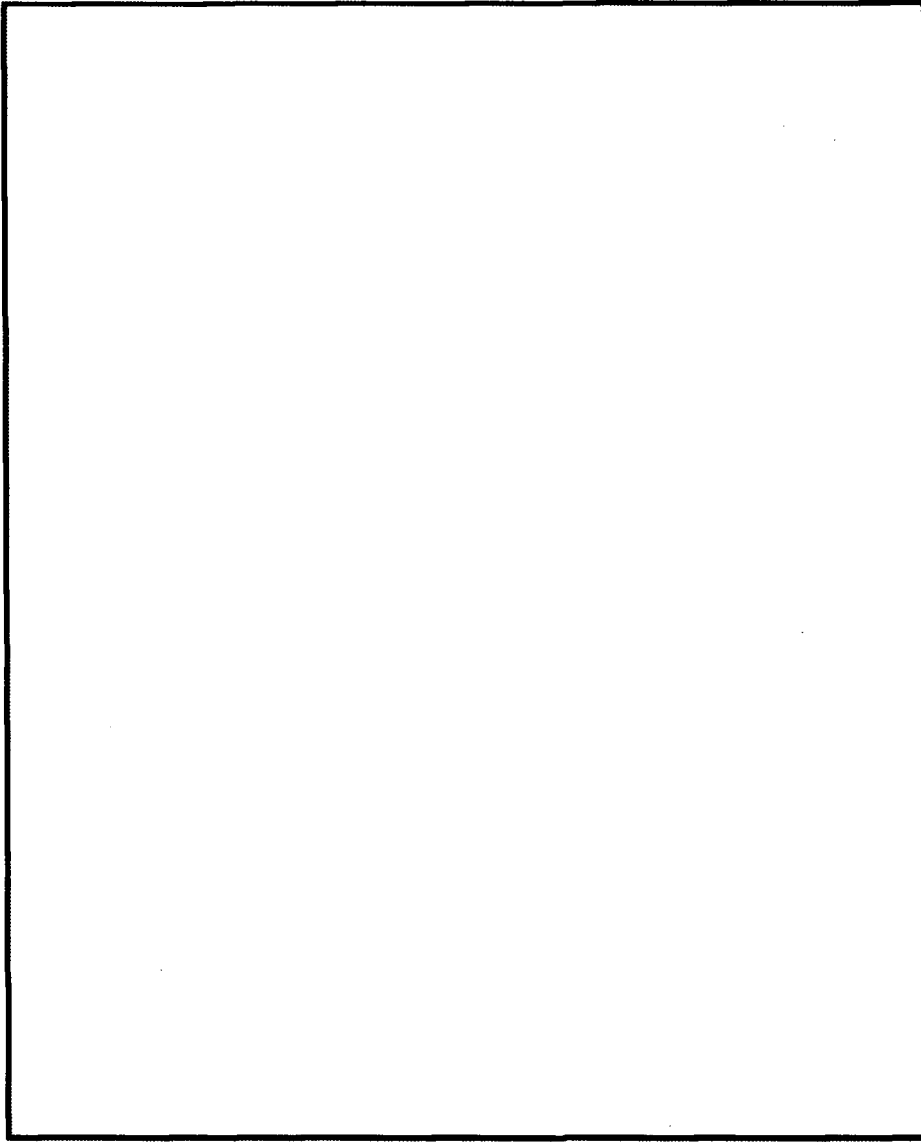


(2)

(b) (3)-P.L. 86-36

(b) (6)

~~FOR OFFICIAL USE ONLY~~



(b) (3) - P.L. 86-36

~~FOR OFFICIAL USE ONLY~~