NSTISSI No. 3026
16 April 1999

(U) OPERATIONAL SECURITY DOCTRINE FOR THE MOTOROLA NETWORK ENCRYPTION SYSTEM (NES)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

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

1. (U) This doctrine establishes the minimum national security standards for handling and control of the Motorola Network Encryption System (NES), its components, and associated key.

2. (U) Comments and suggestions regarding this NSTISSI may be directed to the NSA

3. (U) Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction from the Secretariat at the address listed below.

Michael V. Hayden

MICHAEL V. HAYDEN
Lieutenant General, USAF

NSTISSC Secretariat National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716

(U) OPERATIONAL SYSTEMS SECURITY DOCTRINE FOR THE MOTOROLA NETWORK ENCRYPTION SYSTEM (NES)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

SECTION I - (U) INTRODUCTION

1. (U//~~FOUO~~)

2. (U) **Application** - This document applies to all departments and agencies of the U.S. Government and their contractors who use the NES equipment. Unless otherwise stated, the standards set forth in this document apply to both classified and unclassified NES applications.

3. (U) **Promulgation** - Departments and agencies of the Federal Government must disseminate the information in this document to their subordinate elements and contractors who use NES equipment. Promulgation may be effected by issuing this document or by incorporating its contents in department/agency publications.

4. (U) **Waivers** - Requests for waivers of the provisions of this document must be submitted through appropriate information systems security (INFOSEC) channels to the National Manager, National Security Telecommunications and Information Systems Security (NSTISS).

5. (U) **References** - Documents that are cited as references are listed in ANNEX A.

6. (U) **Definitions** - Selected definitions from National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009 and Federal Standard (FED STD) 1037C are quoted in ANNEX B for reader convenience. Other applicable definitions unique to this NSTISSI are also quoted.

7. (U) **Foreign Release** - Requests for release of the NES to foreign governments must be specifically approved in accordance with existing INFOSEC release policies. Such requests should be forwarded to the NSA

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

8. (U) **Relationship to General Doctrine Documents**

a. (U) **Unkeyed Controlled Cryptographic Items (CCIs)** - NSTISSI No. 4001 states the minimum requirements for safeguarding, controlling, and disposing of unkeyed CCIs, including the NES equipment and their associated fill devices.

b. (U) **Destroying COMSEC Material** - NTISSI No. 4004 prescribes standards for routine destruction of COMSEC material and criteria for protecting COMSEC material under emergency conditions. It also provides guidance and assigns responsibilities for recovery of abandoned COMSEC material.

c. (U) **Key and Keyed CCIs** - NSTISSI No. 4005 states the minimum standards for safeguarding and controlling COMSEC key, including keyed NES equipment and associated fill devices.

d. (U) **Terminal Facilities** - NSTISSI No. 4005 also states the minimum standards for safeguarding COMSEC facilities, including those in which NES equipment are installed.

e. (U) **Controlling Authorities** - NSTISSI No. 4006 states the responsibilities and prerogatives of controlling authorities (CAs) for COMSEC key, including those used on NES-secured nets and circuits.

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

f. (U) **Conflicts with Other Documents**

(1) (U) **Superior Authority** - Except as stated in the next paragraph, when the provisions of this instruction appear to conflict with the provisions of any other national-level issuance, this conflict should be identified and guidance requested, through organizational channels, from the National Manager for NSTISS.

(2) (U//~~FOUO~~)

SECTION II - (U) SYSTEM DESCRIPTION

9. (U//~~FOUO~~)

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

c. (U//~~FOUO~~)

SECTION III - (U) KEYING

10. (U) **Overview** - Effective key management for the NES mandates that the network on which the equipment is used be a LAN, an internetted LAN or a WAN and that it be operated within the parameters discussed in this section.

11. (U//~~FOUO~~)

12. (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

13. (U//~~FOUO~~)

14. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

15. (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

16. (U) **Cryptoperiods**

a. (U//~~FOUO~~)

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

NOTE: (U) NAs may decrease the TEK cryptoperiod during initial configuration of the system.

d. (U//~~FOUO~~)

NOTE: (U) This period may also be decreased by the NA during initial configuration of the system.

17. (U//~~FOUO~~)

18. (U//~~FOUO~~)

SECTION IV - (U) RESTRICTIONS

19. (U) **Compartmented Information** - NES equipment may be used to encrypt compartmented data, provided every person who is authorized access to a keyed NES is .. authorized access to that level of information.

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

20. (U) **Network Classification** - All NES units that intercommunicate must be keyed to the same classification level.

21. (U) **Lower Classified Data** - NES equipment may be used to process data classified lower than that of the communicating network, but such data retains its original classification.

SECTION V - (U) CLASSIFICATION/MARKING/ACCOUNTABILITY

22. (U//~~FOUO~~)

SECTION VI - (U) PHYSICAL SECURITY

23. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

24. (U) Malfunctioning Equipment

a. (U) Alarm Indicators - An alarm condition causes the NES unit's light emitting diode (LED) to illuminate red and an error message and/or error code to be displayed on the unit's LCD.

NOTE: (U) See the **NES Security Platform User's Manual** and **NES System Administration Manual** for details of NES alarm conditions and for a list of error and status messages.

(1) (U) User Action - An NES user is made aware of an NES unit's alarm condition when the user's request for access to the network that the NES serves is denied. In that event, the NA must be notified.

NOTE: (U//~~FOUO~~)

(2) (U//~~FOUO~~)

CAUTION: (U//~~FOUO~~)

b. (U//~~FOUO~~)

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

(3) (U//~~FOUO~~)

c. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(1) (U//~~FOUO~~) [redacted]

(2) (U//~~FOUO~~) [redacted]

(3) (U//~~FOUO~~) [redacted]

(4) (U) **Battery Missing** - The NES LCD indicates "BATTERY LOW" and further investigation reveals that the battery is missing.

NOTE: (U) Whenever the NES LCD indicated "BATTERY LOW," the back-up battery within the NES must be replaced before removing AC power from the unit.

d. (U) **Tampering Not Indicated** - If the physical inspection does not yield any signs of tampering, zeroization of the NES must be attempted and repair completed by authorized maintenance personnel in accordance with the requirements of NSTISSI No. 4000.

25. (U) Unattended Equipment Safeguards

a. (U//~~FOUO~~) [redacted]

b. (U) **Equipment Keyed** - When the NA determines that continuous operation of an NES terminal is operationally required, NES equipment may be left keyed when the terminal area is unmanned, if the area is approved for open storage of material classified at least to the level of key and the facility security officer approves the security measures applied in the terminal area.

NOTE: (U) When authorizing an NES equipment for unattended operation, the NA must reference the appropriate department/agency computer security guidelines and procedures.

NOTE: (U//~~FOUO~~) [redacted]

26. (U) Transportation - The following doctrine applies to the shipment of NES equipment:

a. (U//~~FOUO~~) [redacted]

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

b. (U//~~FOUO~~)

27. (U//~~FOUO~~)

28. (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

29. (U) **Installation**

a. (U) **U.S. Controlled Spaces** - The NES may only be installed in U.S. controlled facilities and spaces worldwide.

NOTE: (U) See NSTISSI No. 4001 for guidance on allowing foreign nationals access to CCIs.

b. (U//~~FOUO~~)

c. (U **Installers** - NES equipment must be installed by authorized U.S. persons or by authorized foreign nationals under continuous supervision by authorized U.S. persons.

d. (U) **Installation Changes** - The NA must be notified of any configuration changes to the network(s) on which NES units are employed.

30. (U) **Safeguarding NES Product Servers/Configuration Managers**

a. (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

program be run on the NPS/CM hard disk drive prior to execution of the NPS/CM software package and at least annually thereafter.

b. (U) **Access and Handling**

(1) (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

(2) (U//~~FOUO~~)

c. (U//~~FOUO~~)

d. (U//~~FOUO~~)

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

e. (U//~~FOUO~~)

31. (U) **Configuration Diskette**

a. (U) **Access and Handling** - Access to an NES configuration diskette must be limited to the NA or his designee, for the purpose of periodically reviewing information on the diskette.

NOTE: (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

b. (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

c. (U) **Storage** - Used or spare NES configuration diskettes should be stored in accordance with their sensitivity, as required by individual department/agency policy.

d. (U//~~FOUO~~)

e. (U) **Disposition** - NES configuration diskettes that are no longer needed must be disposed of in accordance with their classifications; if UNCLASSIFIED, the diskette must be treated as sensitive information.

32. (U) Key

a. (U) **Custodian Responsibilities** - The COMSEC custodian/manager must initially receipt for, account for, and store NES FIREFLY key, until it is hand-receipted to a user.

b. (U) **Access and Handling**

(1) (U) **Operational Key** - Handling of operational key must be commensurate with its indicated classification level, and personnel allowed access to it must hold clearances at least to that level. TOP SECRET operational key must be handled in accordance with two-person integrity procedures outlined in NSTISSI No. 4005.

(2) (U) **Seed Key** - NES seed key must be handled during transportation as UNCLASSIFIED CRYPTO. However, personnel handling seed key that will be converted to classified key must hold clearances commensurate with the level to which the seed key converts.

(3) (U//~~FOUO~~)

[redacted]

(4) (U//~~FOUO~~)

[redacted]

c. (U//~~FOUO~~)

[redacted]

d. (U) **Storage**

(1) (U) **FIREFLY Key** must be stored in accordance with NSTISSI No. 4005.

(2) (U//~~FOUO~~)

[redacted]

e. (U) **Accountability**

(1) (U//~~FOUO~~)

[redacted]

(2) (U//~~FOUO~~)

[redacted]

(3) (U) **CIKs** must be accounted for locally to minimize insecure practices associated with their use. Local accounting involves maintaining a record of all CIKs created, along with the names, organizations/locations of the persons to whom they are issued. In addition, the NA should periodically inventory all CIKs.

f. (U) **Transportation**

(1) (U//~~FOUO~~)

[redacted]

(a) (U)

[redacted]

(b) (U)

(c) (U)

(2) (U//~~FOUO~~)

NOTE: (U)

NOTE: (U//~~FOUO~~)

(3) (U) **Classified Operational Key** - NES classified operational key must be transported by the Defense Courier Service, or designated courier both within and outside the United States.

(4) (U) **CIKs** may be transported on the person of an authorized user or by any means listed above for the shipment of seed key.

CAUTION: (U//~~FOUO~~)

g. (U) **Loss**

(1) (U//~~FOUO~~)

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(2) (U//~~FOUO~~)

(3) (U) **FIREFLY Key** - Loss or compromise of operational FIREFLY key must be reported promptly by the COMSEC custodian/manager, in accordance with NSTISSI No. 4003.

h. (U) **KSD-64A Disposition**

(1) (U//~~FOUO~~)

(2) (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

33. (U//~~FOUO~~)

34. (U//~~FOUO~~)

NOTE: (U//~~FOUO~~)

SECTION VII - (U) REPORTABLE COMSEC INCIDENTS

35. (U) **NSTISSI No. 4003** contains listings of general COMSEC incidents and guidelines for reporting such incidents. The following NES-specific COMSEC incidents must also be reported:

a. (U//~~FOUO~~) **Jeopardizing CIKs** - Failure to adequately protect a CIK that is associated with a lost NES.

b. (U) **Jeopardizing FIREFLY Key** - Loss or suspected compromise of FIREFLY key.

NOTE: (U//~~FOUO~~)

[redacted]

c. (U//~~FOUO~~) [redacted]

d. (U) **Questionable Audit Event** - An audit event that can not be accounted for by the NA.

e. (U//~~FOUO~~) [redacted]

f. (U//~~FOUO~~) [redacted]

g. (U) **Emergency Destruction** - Abandonment of an NES equipment without first destroying its network COMSEC module.

2 Encls:
ANNEX A - References
ANNEX B - Definitions

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

ANNEX A - REFERENCES

(U) This ANNEX is UNCLASSIFIED in its entirety. The following documents, in the order shown, are referenced in this doctrine:

a. **NSTISSI No. 4009,** National Information Systems Security Glossary, dated August 1997.

b. **FED STD 1037C,** General Services Administration, Telecommunications, Glossary of Telecommunications Terms, dated June 1997.

c. **NSTISSI No. 4001,** Controlled Cryptographic Items, dated July 1996.

d. **NTISSI No. 4004,** Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.

e. **NSTISSI No. 4005,** Safeguarding COMSEC Facilities and Material, dated August 1997.

f. **NSTISSI No. 4006,** Controlling Authorities for COMSEC Material, dated 2 December 1991.

g. **NSTISSD No. 502,** National Security Telecommunications and Automated Information Systems Security, dated 5 February 1993.

h. **NSTISSI No. 7000,** TEMPEST Countermeasures for Facilities, dated 29 November 1993.

i. **NES Security Platform User's Manual,** dated 17 May 1995.

j. **NES System Administration Manual,** dated 17 May 1995.

k. **NSTISSI No. 4003,** Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.

l. **NSTISSI No. 4000,** Communications Security Equipment Maintenance and Maintenance Training, dated 1 February 1991.

m. **NSTISSAM TEMPEST/1-92,** Compromising Emanations Laboratory Test Requirements, Electromagnetics, dated 15 December 1992.

n. **NSA Information Systems Security Products and Services Catalog,** revised frequently.

NOTE: Hard copy distribution is soon to be discontinued, but the document is available on the Internet under "http://www.radium.ncsc.mil".

o. **NSTISSAM TEMPEST/2-95,** Red Black Installation Guide, dated 12 December 1995.

ANNEX B - DEFINITIONS

(U) This ANNEX is UNCLASSIFIED in its entirety. Selected definitions from NSTISSI No. 4009 and Federal Standard (FED STD) 1037C are quoted below for reader convenience. Other applicable definitions unique to this NSTISSI are also quoted.

a. **Checksum** - Value computed on data to detect error or manipulation during transmission (NSTISSI No. 4009).

b. **Command Authority** - Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges. (NSTISSI No. 4009).

c. **Controlled Cryptographic Item (CCI)** - Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI". (NSTISSI No. 4009)

d. **Crypto-ignition Key (CIK)** - Device or electronic key used to unlock the secure mode of crypto-equipment. (NSTISSI No. 4009)

e. **Electronic Key Management System (EKMS)** - Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filing, using, and destroying of electronic key and management of other types of COMSEC material. (NSTISSI No. 4009)

f. **Electronic Key Replacement (EKR)** - Function supported by the Electronic Key Management System Central Facility that allows certain identification data in the certificate of each FIREFLY key to be changed electronically. (NSTISSI unique)

g. **Fill Device** - COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment. (NSTISSI No. 4009)

h. **FIREFLY** - Key management protocol based on public key cryptography. (NSTISSI 4009)

i. **FIREFLY KEY** - Electronic key that allows NES equipment to generate per call key. (NSTISSI unique)

j. **Internetted LAN** - Two or more local area networks that communicate across one or more wide area networks. (NSTISSI unique)

k. **Key** - Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in a crypto-equipment for the purpose of encrypting or decrypting electronic signals or for determining electronic counter-counter measures patterns (e.g.,frequency hopping or spread spectrum), or for producing other keys. (NSTISSI No. 4009)

l. **Key Storage Device (KSD)** - Device that can be used as a fill device and also as a crypto-ignition key. (NSTISSI unique)

> **NOTE:** The KSD-64A is used with the NES. When used to key terminals, a KSD-64A is a fill device, and when used to protect key that has been loaded into an NES, it is a CIK.

m. **Local Area Network (LAN)** - A nonpublic data communication system, within a limited geographical area, designed to allow a number of independent devices to communicate with each other over a common transmission-interconnection topology (FED STD 1037C).

n. **Locked Equipment** - NES equipment that either contains no key or from which the crypto-ignition key has been extracted (NSTISSI unique).

o. **NES Administrator** - Individual responsible for overseeing operation of the Motorola Network Encryption System server and for managing the operation of the associated network. (NSTISSI-unique)

p. **Network** - An interconnection of three or more communicating entities. (FED STD 1037C)

q. **Partitioned Security Mode** - Information System (IS) security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an IS. (NSTISSI No. 4009)

r. **Seed Key** - Initial key used to start an updating or key generation process. (NSTISSI No. 4009)

s. **Sensitive Information**, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5. U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1957. Public Law 100-235)

t. **Tampering** - Unauthorized modification altering the proper functioning of IS equipment. (NSTISSI 4009)

u. **TEMPEST** - Short name referring to investigation, study, and control of compromising emanations from INFOSEC equipment. (NSTISSI No. 4009)

v. **Traffic Encryption Key** used to encrypt plain text or to super- encrypt previously encrypted text and/or to decrypt cipher text. (NSTISSI No. 4009)

w. **Unlocked Equipment** - NES equipment containing key and in which the associated crypto-ignition key is inserted. (NSTISSI unique)

x. **User** - Person or process authorized to access an IS. (NSTISSI No. 4009)

y. **User Representative** - Individual authorized by a command authority to order NES FIREFLY key from the Electronic Key Management System Central Facility. (NSTISSI unique)

z. **Wide Area Network (WAN)** - A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks. (FED STD 1037C)

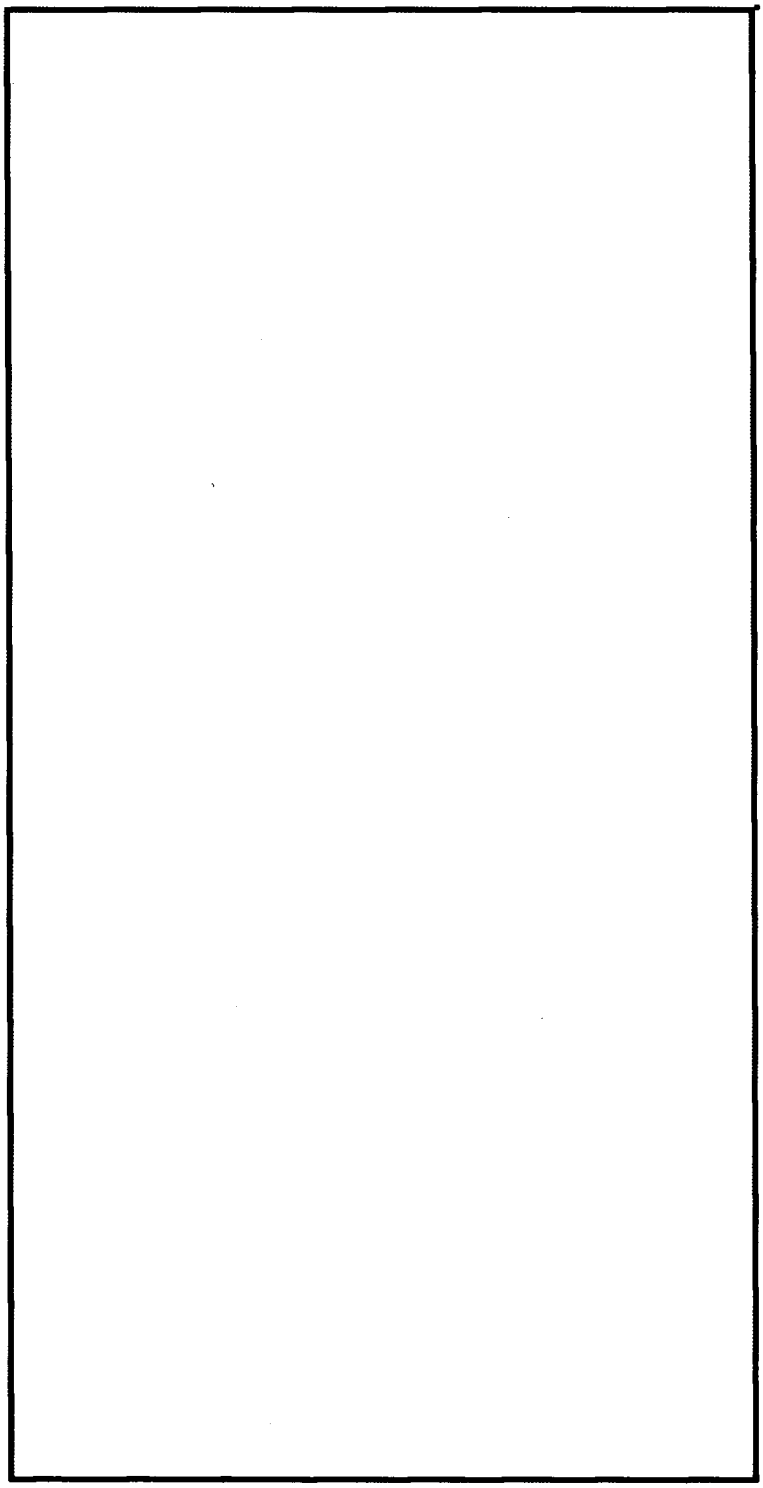
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

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

DISTRIBUTION:

[redacted]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



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