CNSS Instruction No. 3031

(U) OPERATIONAL SYSTEMS SECURITY DOCTRINE FOR THE SECTERA™ IN-LINE NETWORK ENCRYPTOR (KG-235)

This document contains information exempt from mandatory disclosure under the FOIA. Exemption 3 applies.

The information contained herein that is marked U//FOUO is for the exclusive use of the DoD, other U.S. government, and U.S. contractor personnel with a need-to-know. Such information is specifically prohibited from posting on unrestricted bulletin boards or other unlimited access applications, and to an e-mail alias.

This document prescribes minimum standards. Your department or agency may require further implementation.

CNSS Instruction No. 3031

Committee on National Security Systems

6 February 2003

NATIONAL MANAGER

(U) FOREWORD

1. (U) The Committee on National Security Systems Instruction No. 3031, "Operational Systems Security Doctrine for the Sectera™ In-Line Network Encryptor (KG-235)," prescribes the minimum security standards for the protection and use of the KG-235.

2. (U) CNSSI No. 3031 is effective upon receipt. It replaces the Interim Systems Security Doctrine for this equipment, which should be destroyed.

3. (U) Representatives of the Committee on National Security Systems may obtain additional copies of this Instruction at the address listed below.

4. (U) U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

5. (U//~~FOUO~~) Comments and suggestions regarding this Instruction may be sent directly to the National Security Agency [redacted]

MICHAEL V. HAYDEN
Lieutenant General, USAF

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

CNSS Secretariat [redacted], National Security Agency, 9800 Savage Road STE 6716, Ft Meade MD 20755-6716
[redacted]

(U) OPERATIONAL SYSTEMS SECURITY DOCTRINE FOR THE SECTERA™ IN-LINE NETWORK ENCRYPTOR (KG-235)

TITLE **SECTION**

PURPOSE AND SCOPE....................I
REFERENCES....................II
DEFINITIONS....................III
EQUIPMENT/SYSTEM DESCRIPTION/LEVEL OF USE....................IV
PERSONNEL RESPONSIBILITIES....................V
KEYING INFORMATION....................VI
CLASSIFICATION/MARKING....................VII
SECURITY AUDIT LOG....................VIII
CONTROL REQUIREMENTS....................IX
MAINTENANCE....................X
DISPOSITION/DESTRUCTION....................XI
COMSEC INCIDENTS, REPORTING, AND EVALUATION....................XII
EXCEPTIONS....................XIII

SECTION I - (U) PURPOSE AND SCOPE

1. (U) This doctrine contains minimum security standards for the protection and use of the [1]Sectera™ In-Line Network Encryptor (INE) (KG-235) equipment, its associated components, and Communications Security (COMSEC) material.

2. (U) The provisions of this doctrine apply to all departments and agencies of the U.S. Government and their contractors who handle, distribute, account for, store, or use the Sectera INE and its associated COMSEC material.

3. (U) Any conflicts between the requirements contained in this doctrine and any other national-level publication shall be identified and submitted for resolution to the Director, National Security Agency (DIRNSA), Information Assurance (IA) [redacted] However, this does not preclude any department or agency of the U.S. Government from applying more stringent security measures to their equipment than this doctrine requires.

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

SECTION II - (U) REFERENCES

4. (U) This doctrine makes reference to a number of other national-level documents. A listing of these documents is contained in ANNEX A.

[1] Sectera™ is a trademark of the General Dynamics Corporation

SECTION III – (U) DEFINITIONS

5. (U) Definitions and acronyms contained in the references listed in ANNEX A apply to this doctrine. Additional definitions of specialized terms that are unique to this doctrine are contained in ANNEX B.

SECTION IV - (U) EQUIPMENT/SYSTEM DESCRIPTION/LEVEL OF USE

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

7. (U) Throughput - The maximum throughput of the Sectera INE equipment is 20 Mbps.

8. (U) Sectera INE System Components - The Sectera INE system comprises a KG-235 equipment, a KSD-64A Key Fill Device/Crypto-Ignition Key (CIK), a JOSEKI KSD-64A, and an INE Configuration Manager (CM).

9. (U) Keying Material

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

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

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

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

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

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

SECTION V – (U) PERSONNEL RESPONSIBILITIES

12. (U) Network Administrator - The Network Administrator (NA) is responsible for the network and security configuration of all Sectera INE equipment within the NA's domain. Specifically, the NA is responsible for the following functions:

a. (U) Net planning; and

b. (U) Requesting generation of FIREFLY credentials from the Central Facility (CF).

13. (U) Security Administrator - The Security Administrator (SA) is responsible for maintaining, monitoring, and controlling all security functions performed by the Sectera INE equipment. The SA also interfaces with both the COMSEC Custodian and the NA for management of keying material. The SA is the only individual who may fill key and initialize CIKs. Since the SA configures the security functions of the Sectera INE, this individual must be knowledgeable of all Sectera INE security functions. Local security policy may dictate the number of individuals assigned the role of SA. The SA is responsible for the following:

a. (U) Receipting for all Sectera INE key from the COMSEC custodian;

b. (U) Physical keying and rekeying of Sectera INE equipment, including ensuring that each key is filled into the appropriate/approved Sectera INE equipment;

c. (U) Setting the Sectera INE clock;

d. (U) Ensuring that only approved procedures are followed for the storage, protection, and local accounting of Sectera INE key;

e. (U) Notifying the COMSEC Custodian of incidents/insecurities affecting Sectera INE material and ensuring recovery actions are taken, when appropriate;

f. (U) Tamper recovery;

g. (U) Performing zeroization of Sectera INE equipment and/or disposal of CIKs; and

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

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

[redacted]

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

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

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

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

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

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

SECTION VI - KEYING INFORMATION

17. (U) Controlling Authority - Reference b establishes the responsibilities of organizations that serve as controlling authorities for COMSEC keying material, and provides guidance for fulfilling those responsibilities.

18. (U) Key Distribution - All keying material will be distributed through the EKMS. Use of the KSD-64A will be the normal means of filling operational key into the Sectera INE equipment. The ordering, generation, and distribution of Sectera INE key will follow established EKMS and COMSEC Material Control System (CMCS) doctrine.

19. (U) Types of Key

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

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

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

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

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

20. (U) Cryptoperiods

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

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

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

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

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

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

21. (U) Alarms - Sectera INE equipment does not contain an audible alarm feature. The operator must watch for the Alarm Light Emitting Diode (LED) indicator to light. An error message and/or error code will be displayed on the unit's liquid crystal display (LCD).

a. (U) The SA should attempt to clear an alarm condition according to the guidelines provided in the Sectera INE User's Manual. If the alarm condition can be cleared by the SA, the Sectera INE may be reinitialized, which requires the Operational CIK to be removed and reinserted to resume operation. The SA should then review the audit events record.

b. (U) If the alarm condition cannot be cleared by the SA, a physical inspection must be performed and the vendor contacted for additional service.

c. (U) If the error condition displayed indicates failed zeroization or tamper, the Sectera INE should be considered to be tampered and must be immediately taken out of service. The event should be reported as a COMSEC Incident.

SECTION VII - CLASSIFICATION/MARKING

22. (U) Reference c. provides general classification guidance for COMSEC information. The following additional guidance also applies:

a. (U) The Sectera INE equipment is an UNCLASSIFIED/Controlled Cryptographic Item (CCI) when unkeyed.

b. (U) When keyed, it is classified at the classification level of the key it contains and must be protected accordingly.

NOTE: (U) For the purpose of this document, a keyed Sectera INE is a Sectera INE with key filled and a CIK inserted. If key is filled but the CIK is removed and properly stored, the Sectera INE is considered unkeyed.

c. (U) The JOSEKI KSD-64A is SECRET.

23. (U) ANNEX C contains a summary of the classification and handling of Sectera INE keying material and equipment.

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

SECTION VIII - SECURITY AUDIT LOG

24. (U) Audit Log

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

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

SECTION IX - CONTROL REQUIREMENTS

25. (U) Control Requirements - The Sectera INE equipment is UNCLASSIFIED/CCI when unkeyed and must be handled as such. Reference d. prescribes the minimum national standards for safeguarding and control of classified COMSEC equipment and COMSEC keying material. Individuals requiring access to Sectera INE equipment must possess an appropriate U.S. Government security clearance and must have a need-to-know for the equipment. Reference d. also prescribes the minimum national standards for safeguarding COMSEC facilities operated by the U.S. Government or by contractors in connection with U.S. Government contracts.

26. (U) Reference e. prescribes the minimum national standards for handling and control of unkeyed CCI equipment and components.

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

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

a. (U) When the CIK is stored in the same room as the equipment, the CIK must be afforded protection commensurate with the classification of the keyed equipment (e.g., in an approved security container). The CIK may also be stored in an area separate from the room in which the

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

equipment is located under the best conditions available (e.g., a locked cabinet or desk may be sufficient).

b. (U) CIKs used during normal operations must be protected against unauthorized access and use. Prescribed controls are not needed for CIKs used in equipment filled with test key.

c. [redacted]

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

a. (U) The CM workstation must be a stand-alone workstation or reside on a network dedicated to network management functionality. The CM workstation may not be used for general-purpose computing or reside on a general-purpose network.

b. (U) Password protection on the CM workstation is required.

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

d. (U) The Sectera INE also supports unprotected SNMP management from either the RED or BLACK side. No doctrinal restrictions currently exist; however, the user should refer to the Security Features User's Guide for possible risks introduced when this service is used.

30. (U) Accountability

a. (U) The Sectera INE equipment must be accounted for by its serial number. If this equipment is controlled in the COMSEC Material Control System, it shall be assigned Accounting Legend Code (ALC) 1. Detailed accounting requirements for CCI equipment are contained in reference e.

b. (U) Accountability Requirements for Sectera INE Keying Material:

(1) (U) All FFVS material is assigned ALC-1 (if in physical form, e.g., on a KSD-64) or ALC-6 (if in electronic form, e.g., in a Data Transfer Device (DTD)) and shall be accounted for in accordance with requirements contained in reference d.

(2) (U) All FFVS material is accountable by registration number until actually loaded into the Sectera INE equipment. The operational key is marked CRYPTO and may range from UNCLASSIFIED to TOP SECRET.

(3) (U) Keying material used in classroom training only shall be test key and shall be marked UNCLASSIFIED/CRYPTO. It may be used indefinitely. It is accounted for as ALC-4.

c. (U) CIKs must be accounted for locally. Local accounting is done by the SA. With respect to the CIKs, the local accounting procedures must include a record of all CIKs along with the names and organizations/locations of the persons to whom they are issued. In addition, a responsible person must inventory the CIKs semi-annually and upon appointment of a new SA.

d. (U) JOSEKI KSD-64As must be accounted for locally.

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

32. (U) Transportation

a. (U) The Sectera INE is CCI and may be shipped by any method described in reference e. Sectera INEs shall be shipped in zeroized state with batteries in place. Shipping requirements for malfunctioning equipment are described in the maintenance section below.

b. (U) CIKs must be transported on the person of an authorized operator. When they must be shipped, they shall be handled through U.S.-controlled postal systems, preferably by U.S. Registered Mail. CIKs must always be shipped separately from their associated equipment, except when the equipment has been zeroized as noted in paragraph 36, below.

c. (U) JOSEKI KSD-64As must be shipped separately from the equipment and must be protected at the SECRET level.

SECTION X - MAINTENANCE

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

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

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

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

[redacted]

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

SECTION XI - DISPOSITION/DESTRUCTION

36. (U) Zeroization

a. (U) Active (panic) zeroization of all key in the Sectera INE equipment is accomplished from the equipment's front panel by activating the double action zeroization switch. Any attempt to tamper with the equipment also results in complete zeroization;

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

37. (U) Disposition/Destruction of E-HRL Circuit Card Assemblies (CCA)

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

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

(1) (U)

(2) (U)

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

(3) (U) [redacted]

(4) (U) [redacted]

(5) (U) [redacted]

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

SECTION XII - COMSEC INCIDENTS, REPORTING, AND EVALUATION

38. (U) COMSEC Incident Reports must be submitted to DIRNSA [redacted] using the standard reporting channels established within each department or agency. Reference i. contains a general listing of reportable COMSEC incidents and the standards for reporting them. Additional reportable COMSEC incidents specific to Sectera INE follow:

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

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

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

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

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

f. (U) Shipment of keyed equipment without having obtained prior authorization from the appropriate central authority for that equipment.

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

39. (U) Insecure Practices - The following occurrences are insecure practices which need not be reported to NSA unless there is an indication of espionage or sabotage. Such occurrences should, however, be monitored and evaluated within each using organization for possible follow-up action.

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

b. (U) Loss of any CIK - Loss of a CIK should be promptly reported to the SA, who should immediately zeroize the Sectera INE. In addition, an "Insecure Practice" Report must be submitted through department or agency channels for appropriate action.

SECTION XIII - EXCEPTIONS

40. (U) Exceptions - Requests for exceptions to any of the provisions of this doctrine must be approved, on a case-by-case basis, prior to implementation. Each request shall include a complete operational justification and shall be submitted through appropriate department or agency channels to DIRNSA, IA Policy, Procedures, and Insecurities Division (I41) for review.

3 Encls:
1. ANNEX A - References
2. ANNEX B - Definitions of Specialized Terms
3. ANNEX C - TABLE, Classification and Handling of Sectera INE (KG-235) Keying Material and Equipment

ANNEX A

REFERENCES

1. (U) The information contained in this ANNEX is UNCLASSIFIED in its entirety.

2. (U) The following national-level documents are referenced in this operational systems security doctrine.

a. (U) NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated September 2000.

b. (U) NSTISSI No. 4006, Controlling Authorities for COMSEC Material, dated 2 December 1991.

c. (U) NTISSI No. 4002, Classification Guide for COMSEC Information, dated 5 June 1986.

d. (U) NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, dated August 1997.

e. (U) NSTISSI No. 4001, Controlled Cryptographic Items, dated July 1996.

f. (U) NSTISSI No. 7000, Tempest Countermeasures for Facilities, dated 29 November 1993. (Document is classified CONFIDENTIAL)

g. (U) NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, dated January 1998.

h. (U) NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.

i. (U) NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.

ANNEX B

DEFINITIONS OF SPECIALIZED TERMS

a. (U) Command Authority – Individual responsible for the appointment of user representatives for a department, agency, or organization, and for their key ordering privileges. The CA will also be responsible for setting up and managing closed partitions and assigning privileges to User Representatives to order keying material.

b. (U) Electronic Key Management System (EKMS) – An interoperable collection of systems being developed by Services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material (NSTISSI 4009). The EKMS is the national source of FIREFLY Keying Material.

c. (U) FIREFLY Keying Material – Also referred to as FIREFLY Vector Set, this is the keying material used to generate a FIREFLY TEK between peer Sectera INEs.

d. (U) FIREFLY Traffic Encryption Keys (TEK) – This is the keying material that is generated during a FIREFLY Exchange between peer Sectera INEs and is used to encrypt/decrypt data passing through the Sectera INE.

e. (U) Keyed Sectera INE – A Sectera INE that has been filled with keying material and in which the associated CIK has been inserted. This is equivalent to "unlocked."

f. (U) Key Storage Device (KSD) – A physical device that can be used as a fill device and also as a Crypto Ignition Key (CIK). It is a small device shaped like a physical key and contains passive memory. When it is used to carry key to terminals, it is termed a fill device. When it is used to protect key that has been loaded into terminals, it is a CIK. KSD-64A is the nomenclature of the physical device used to provide keying material for the Sectera INE.

g. (U) Network Administrator (NA) - The individual who is responsible for the definition, modification, selection, deletion, and management of a network consisting of intercommunicating Sectera INE and possibly NES equipment. This term applies to the NA and other personnel designated by the NA.

h. (U) Partition – A subgroup of users who wish to communicate exclusively among themselves. Inclusion/Exclusion in the group is enforced by a partition code in the FFVS.

i. (U) Security Administrator (SA) - The individual(s) responsible for maintaining, monitoring, and controlling functions performed by the Sectera INE equipment.

j. (U) Universal – A subset of cryptographic material contained in the FFVS used to segregate users. Devices must have key with the same universal to communicate.

k. (U) Unkeyed Sectera INE – A Sectera INE in which no key has been filled or in which key has been filled but CIK is removed. This is equivalent to "locked."

l. (U) User Representative - An individual authorized by a Command Authority to order FIREFLY key material from the EKMS-CF. This individual may or may not be the COMSEC Custodian.

ANNEX C

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

(U) CLASSIFICATION AND HANDLING OF

SECTERA INE (KG-235) KEYING MATERIAL AND EQUIPMENT

[redacted]

This Table shall be handled as For Official Use Only material.

DISTRIBUTION:

[redacted]

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