NSTISSI No. 3019
30 October 2001

(U) OPERATIONAL SYSTEMS SECURITY DOCTRINE FOR THE FASTLANE (KG-75 AND KG-75A)

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

National Security Telecommunications and Information Systems Security Committee

NSTISSI No. 3019

National Manager

FOREWORD

1. (U) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3019, *Operational Systems Security Doctrine for the FASTLANE (KG-75 and KG-75A)*, prescribes minimum security standards for the protection and use of the KG-75 and KG-75A high-speed encryption devices.

2. (U) NSTISSI No. 3019 is effective upon receipt. It replaces the Interim Systems Security Doctrine for the FASTLANE (KG-75), dated 23 October 2000, which should be destroyed.

3. (U) Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this NSTISSI 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~~) [redacted]

Michael V. Hayden

MICHAEL V. HAYDEN
Lieutenant General, USAF

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

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

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

NSTISSI No. 3019

(U) OPERATIONAL SYSTEMS SECURITY DOCTRINE FOR THE FASTLANE (KG-75 and KG-75A)

SECTION I - (U) PURPOSE AND SCOPE

1. (U) This doctrine contains minimum security standards for the protection and use of the FASTLANE equipment. to include all releases. its associated components. and Communications Security (COMSEC) material.

2. (U) 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 FASTLANE 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). [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.

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.

[redacted] (b)(3)-P.L. 86-36

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

SECTION III - (U) DEFINITIONS

5. (U) Definitions and acronyms contained in Reference 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~~)

7. (U) Throughput - FASTLANE is capable of processing up to 4096 virtual channel connections, with each channel processing information at the same security classification level.

8. (U//~~FOUO~~)

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

10. (U//~~FOUO~~)

a. (U) Reference b sets forth minimum security standards for safeguarding, controlling, and using the LMD/KP.

b. (U) Reference c sets forth minimum security standards for the protection and use of the DTD.

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

SECTION V - (U) PERSONNEL RESPONSIBILITIES

12. (U) Local Authority - The Local Authority (LA) is responsible for the network and security configuration of all the FASTLANE equipment within the LA's domain. Specifically, the LA is responsible for the following functions:

a. (U) net planning; and

b. (U) specifying FIREFLY credentials.

13. (U) Security Administrator (SA) - The SA is responsible for the network and security configuration of all the FASTLANE equipment within the SA's domain. Specifically, the SA is responsible for the following functions:

a. (U) performing initialization and distribution of CIK Cards to users, to include keeping a record of the serial number of each CIK Card, to whom it is issued and the serial number of the FASTLANE equipment with which it is associated:

NOTE: (U) Since CIK Cards do not come with a serial number, the SA must mark the cards with identification numbers. A possible means is to use the serial number of the associated FASTLANE equipment plus an additional unique number for each CIK associated with that FASTLANE equipment.

b. (U) receipting for all FASTLANE key from the COMSEC Custodian:

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

d. (U) ensuring that only approved procedures are followed for the storage, protection, and local accounting of FASTLANE key:

e. (U) notifying the COMSEC Custodian of incidents/insecurities affecting FASTLANE material and when appropriate, ensuring recovery actions are taken:

f. (U~~//FOUO~~)

g. (U~~//FOUO~~)

h. (U) approving and witnessing the opening of the FASTLANE equipment:

i. (U) generating Tamper Key on site:

j. (U) performing software download; and

k. (U) storing and accounting for all Master and Registration Cards as well as SWDL Image and Decrypt Cards.

14. (U) COMSEC Custodian - The COMSEC Custodian is responsible for the normal duties of a COMSEC Custodian, as well as providing the interface with both NSA for FIREFLY Key Sets and the key generation element for preplaced (traditional) key. Depending upon local conditions, the functions of the LA and SA may be combined and vested in one individual. The role of COMSEC Custodian may also be combined with one or both of these roles.

15. (U//FOUO)

SECTION VI - (U) KEYING INFORMATION

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

17. (U) Key Distribution - All keying material will be distributed via the Electronic Key Management System (EKMS). Use of the DTD will be the normal means of filling key into the FASTLANE equipment. The ordering, generation, and distribution of FASTLANE key will follow established EKMS and COMSEC Material Control System (CMCS) doctrine.

18. (U) Types of Key

a. (U//FOUO)

b. (U//FOUO)

c. (U//FOUO)

d. (U//FOUO)

e. (U//FOUO)

NOTE: (U//FOUO)

19. (U//~~FOUO~~)

20. (U//~~FOUO~~)

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

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

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

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

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

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

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

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

f. (U//~~FOUO~~)

g. (U//~~FOUO~~)

21. (U//FOUO)

NOTE: (U//FOUO)

22. (U) Alarms - FASTLANE equipment does not contain an audible alarm feature. The user must watch for the Alarm Light Emitting Diode (LED) indicator to light. An alarm message will be displayed in the status area, which is the top line of both the front panel and the maintenance terminal.

SECTION VII – (U) CLASSIFICATION MARKING

23. (U) Classification Guidance - Reference e provides general classification guidance for COMSEC information. The following additional guidance also applies:

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

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

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

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

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

e. (U//FOUO)

f. (U//FOUO)

g. (U) CIK Card - The CIK Card is UNCLASSIFIED.

h. (U) Software Download (SWDL) Image Card - The Software Download Image Card is UNCLASSIFIED.

i. (U//FOUO)

24. (U) Security Administrator Personnel Identification Number (SA PIN) - The SA PIN is UNCLASSIFIED and shall be protected in accordance with existing site procedures designed to protect against access by unauthorized individuals. The SA PIN should be recorded and appropriately safeguarded since each equipment will have a separate SA PIN generated by the equipment. Loss of the SA PIN requires zeroization and rekeying of the equipment.

25. (U) Remote Locations - In the case of video remoting of the FASTLANE's front panel. the image data must be protected to the same degree as the signal line between the configuration maintenance terminal and the remote FASTLANE (see paragraph 23c. above).

26. (U) Classification and Handling Chart - ANNEX D contains a summary of the classification and handling of FASTLANE keying material and equipment.

SECTION VIII - (U) SECURITY AUDIT LOG

27. (U) Audit Log - At least once a month. the SA shall read the FASTLANE security audit log. However. the security audit log must be read immediately if the log capacity reaches 80% full or the audit function will default to logging only security critical events. The user will be notified capacity has been reached by the illumination of the alarm LED and a status message on the front panel and active Human Machine Interface (HMI). It is suggested that this log be retained (off-line from the FASTLANE equipment) for a period of time that is adequate for use in investigating potential security violations. The length of time to retain the security audit log will be determined locally or by the parent department or agency. The security audit log may be retained in physical form (by use of the configuration maintenance terminal's print screen function) or in electronic form (using a smart terminal with the capability of downloading to a disk).

a. (U//FOUO)

b. (U) The security audit log has three modes:

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

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

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

SECTION IX - (U) CONTROL REQUIREMENTS

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

29. (U//~~FOUO~~)

30. (U//~~FOUO~~)

31. (U) Facilities - Reference f 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.

32. (U//~~FOUO~~)

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

33. (U) Storage and Handling

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

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

c. (U) Master Card - The Master Card must be secured in the same manner as a CIK Card. A back-up copy may be kept in case of a PCMCIA Card battery failure.

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

34. (U) Accountability

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

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

35. (U) Transportation

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

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

36. (U//~~FOUO~~)

SECTION X - (U) MAINTENANCE

37. Maintenance - Reference i establishes minimum standards, delineates responsibilities, and establishes procedures for COMSEC equipment maintenance and maintenance training. In addition, the following specific requirements also apply with respect to the FASTLANE equipment:

a. (U) An authorized individual, trained in field-level maintenance, may open the FASTLANE equipment and replace printed circuit boards. After doing this, the SA must generate a new Tamper Key. Therefore, the SA must pre-approve all instances when the equipment is to be opened. The SA must be present both when the FASTLANE equipment is opened to ensure that the equipment does not already indicate a tamper at that point, and then when the FASTLANE equipment is closed to ensure that no unauthorized parts have been introduced into the equipment. The SA shall subsequently generate the Tamper Key.

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

38. (U//~~FOUO~~)

39. (U) Batteries

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

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

40. (U//~~FOUO~~)

SECTION XI - (U) DISPOSITION/DESTRUCTION

41. (U) Zeroization

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

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

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

42. (U) Destruction Guidance and Protection - Reference j prescribes minimum national standards for routine destruction of COMSEC material, and provides criteria and guidance for protecting COMSEC material under emergency conditions. It also provides guidance and assigns responsibilities for recovery of abandoned COMSEC material.

SECTION XII - (U) COMSEC INCIDENTS/ADMINISTRATIVE INCIDENTS

43. (U//~~FOUO~~)

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

(1) (U) the equipment is found and zeroized;

(2) (U) the CIK is deleted from that equipment or destroyed; or

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

(U//~~FOUO~~)

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

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

d. (U) Tampering - Any suspected tampering, including that due to:

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

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

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

44. (U) Reportable COMSEC Incidents - The following incidents involving the FASTLANE Releases 1, 2, or 3 and higher equipment shall be reported to the Director, NSA, in accordance with requirements set forth in Reference g:

a. (U) evidence of tampering with or unauthorized access to the equipment:

b. (U) known or suspected theft of an unkeyed equipment: or

c. U) shipment of a keyed equipment without having obtained prior authorization from the appropriate central authority for that equipment.

45. (U) Administrative Incidents - The following occurrences are insecure practices that need not be reported to DIRNSA 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~~)

b. (U) Loss of any CIK - Loss of a CIK should be promptly reported to the SA, who should immediately ensure deletion of that CIK from the specific FASTLANE equipment with which it was associated. In addition, an Insecure Practice Report must be submitted through department or agency channels for appropriate action.

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

SECTION XIII - (U) EXCEPTIONS

46. (U//~~FOUO~~)

3 Encls:
1. ANNEX A - References
2. ANNEX B - Definitions of Specialized Terms
3. ANNEX C - TABLE Classification and Handling of the FASTLANE Key and Equipment

ANNEX A
(U) REFERENCES

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

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

b. (U) NAG No. 71. Interim Operational Systems Security Doctrine for the Local Management Device/Key Processor (LMD/KP) (KOK-22). dated April 1997.

c. (U) NSTISSI No. 3021. Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device (DTD). dated September 1997.

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

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

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

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

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

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

j. (U) NSTISSI No. 4004. Routine Destruction and Emergency Protection of COMSEC Material. dated 11 March 1987. (Document is classified CONFIDENTIAL.)

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

ANNEX B
DEFINITIONS OF SPECIALIZED TERMS

a. (U) Local Authority - That individual responsible for the network and security configuration of all the FASTLANE equipment within his/her domain.

b. (U) Master Card - A PCMCIA Card used in conjunction with the Registration Card to perform a cold start of the FASTLANE equipment. In the FASTLANE Release 1 and 2, the Master Card is converted to the Master CIK.

c. (U) Master CIK - A PCMCIA Card that is created by the user during the cold start process. In the FASTLANE Release 1 and 2 it is created by converting the Master Card. In the FASTLANE Release 3, this additional PCMCIA Card is provided with the unit and the Master CIK is created by the user. The Master CIK is used to warm start the FASTLANE to transition to operational state and unlock the Firefly Key Sets and/or replaced TEKs associated with the CIK.

d. (U) Registration Card - A PCMCIA Card used in conjunction with the Master Card to perform a cold start of the FASTLANE equipment.

e. (U) Security Administrator - That individual responsible for maintaining, monitoring, and controlling functions performed by the FASTLANE equipment.

f. (U) Software Download (SWDL) Decrypt Card - A PCMCIA Card that contains information required to decrypt the software images from the SWDL Image Card during the trusted software download process.

g. (U) Software Download (SWDL) Image Card - A PCMCIA Card that contains encrypted and signed software images to be loaded into the FASTLANE using the trusted software download process.