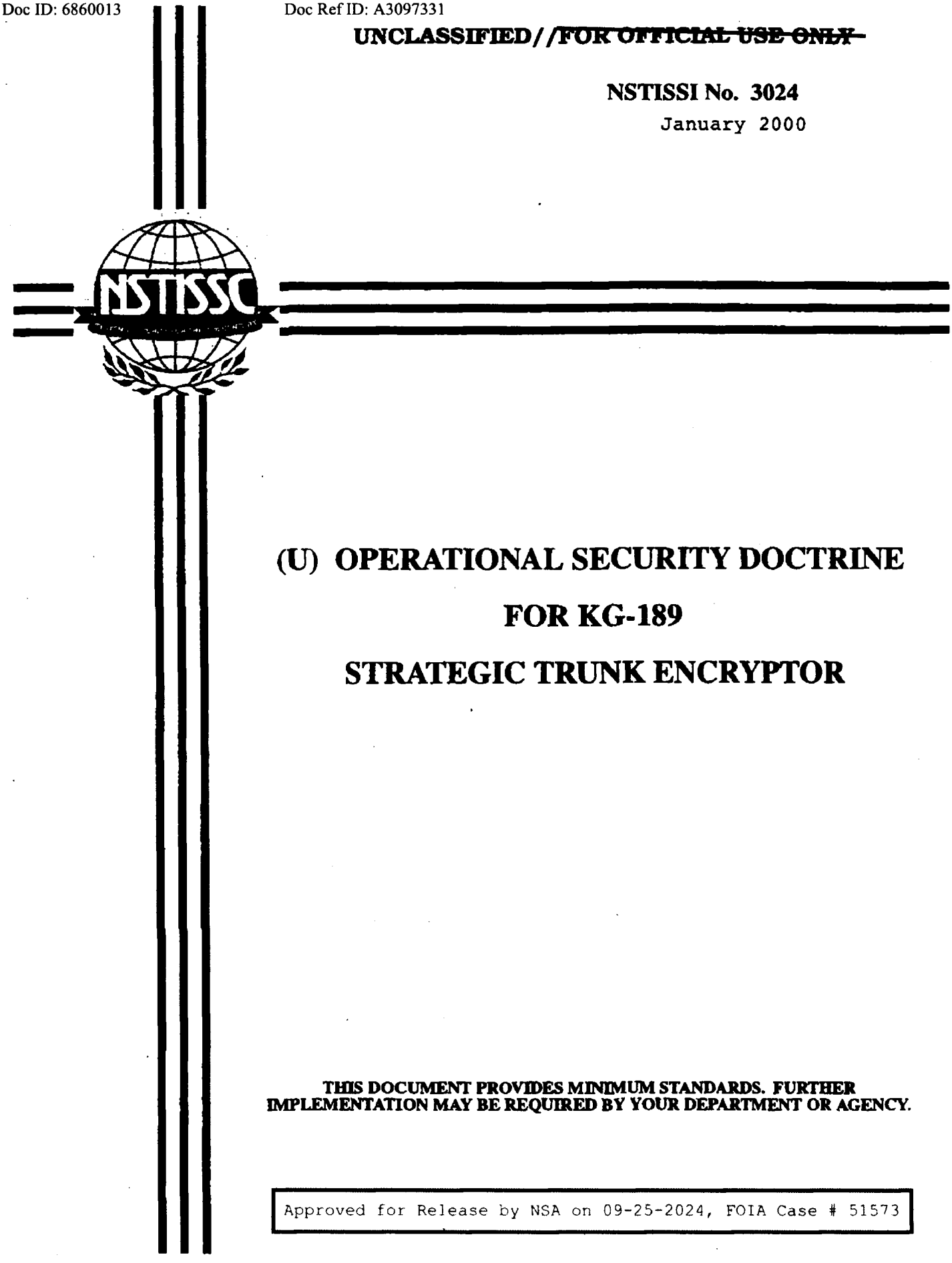
NSTISSI No. 3024
January 2000



(U) OPERATIONAL SECURITY DOCTRINE FOR KG-189 STRATEGIC TRUNK ENCRYPTOR

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

1. This doctrine establishes the minimum national security standards for safeguarding, controlling, and using the KG-189 and its associated key.

2. Comments and suggestions regarding this NSTISSI may be directed to the NSA [redacted] telephone [redacted]

3. 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.

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

MICHAEL V. HAYDEN
Lieutenant General, USAF

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

[redacted]

(U) OPERATIONAL SECURITY DOCTRINE FOR KG-189 STRATEGIC TRUNK ENCRYPTOR

TITLE SECTION

SECTION I - (U) INTRODUCTION

1. (U) Purpose - This doctrine expresses the minimum security standards for safeguarding, controlling, keying, and using the KG-189 and its associated key.

2. (U) Application - This doctrine applies to the departments and agencies of the U.S. Government and their contractors who use or hold the KG-189. It supersedes doctrine expressed in National Security Agency (NSA) memorandum Subject: Test Security Doctrine for the KG-189 Strategic Network Encryptor, dated 11 April 1996.

3. (U) Waivers - Requests for exceptions to any of the provisions of this document must be submitted through department/agency channels to the National Manager for Information Systems Security (INFOSEC) ATTN: National Security Agency (NSA) Policy, Procedures, and Insecurities Division.

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

NOTE: (U) The NSA may be reached at DSN

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

5. (U) References cited in this document are identified in ANNEX A.

6. (U) Definitions - Selected definitions from NSTISSI No. 4009 and FED-STD-1037C are quoted in ANNEX B, and one system-unique term is also defined therein.

7. (U) Acronyms - A listing of KG-189 related acronyms and their expansions is presented in ANNEX C.

8. (U) Relationship to General Doctrine - The following general doctrine applies to the communications security (COMSEC) material associated with the KG-189 system:

a. (U) **NSTISSI No. 4000** establishes minimum standards, delineates responsibilities, and establishes procedures for COMSEC equipment maintenance and maintenance training.

b. (U) **NSTISSI No. 4001** sets forth the minimum requirements for controlling

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

unkeyed controlled cryptographic item (CCI) equipment and components.

c. (U) **NSTISSI No. 4002** provides general guidance relative to the classification of COMSEC information.

d. (U) **NSTISSI No. 4003** contains a general listing of reportable COMSEC incidents and standards for reporting them.

e. (U) **NSTISSI No. 4004** prescribes 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.

f. (U) **NSTISSI No. 4005** describes the minimum standards for safeguarding and controlling keying material and establishes additional controls that apply when CCI (and/or classified) equipment is keyed. It also prescribes standards for safeguarding COMSEC facilities operated by the U.S. Government or by contractors in connection with U.S. Government contracts.

g. (U) **NSTISSI No. 4006** describes responsibilities of organizations that serve as controlling authorities for key and provides guidance for accomplishing those responsibilities.

h. (U) **NSTISSI No. 7000** establishes guidelines, restrictions, and procedures for determining the applicable TEMPEST countermeasures for equipment, systems, and facilities that process national security information.

9. (U) **Conflicts with Other Documents** - Any conflicts between this doctrine and other published national level doctrine should be brought to the attention of the National Manager for INFOSEC ATTN: NSA INFOSEC Policy, Procedures, and Insecurities Division for resolution.

SECTION II - (U) SYSTEM DESCRIPTION

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

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

SECTION III - (U) KEYING

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

13. (U) Types of Key

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

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

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

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

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

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

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

14. (U) **Loading FIREFLY Key**

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

a. (U) **Loading Methods**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. (U) Cryptoperiods

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

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

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

16. (U~~//FOUO~~)

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

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

SECTION IV - (U) CLASSIFICATION/MARKING/ACCOUNTABILITY

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

SECTION V - (U) SOFTWARE UPDATING

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

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

SECTION VI - (U) PHYSICAL & PERSONNEL SECURITY

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

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

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

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

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

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

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

(5) (U~~//FOUO~~)

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

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

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

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

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

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

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

[redacted]

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

20. (U) **Operator Access**

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

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

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

21. (U) **Storage** - Uninstalled, unkeyed KG-189 equipment and their E-HII E-HIH, and E-HYZ circuit boards are controlled cryptographic items (CCIs) that must be stored as high-value Government property in accordance with NSTISSI No. 4001.

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

23. (U) **Installation & Maintenance**

a. (U) **Installation** - KG-189s must be installed in fixed COMSEC facilities, as defined in NSTISSI No. 4005.

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

c. (U) **Maintenance Personnel** - KG-189 maintenance must be performed by qualified persons who are U.S. citizens cleared to the classification level of the installed FIREFLY key. If a KG-189 that has been released for use by a foreign nation or international organization becomes inoperative, it must be returned to a U.S. activity for maintenance.

24. (U) **Transportation**

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

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

25. (U) **Safeguarding Unattended Terminals** - Keyed KG-189s may be left in U.S. controlled, unmanned terminal areas if any of the following conditions are met:

a. (U//~~FOUO~~) **Open Storage** - If the terminal area has been approved by the responsible facility security officer for open storage of information classified at least to the level of the key being used.

b. (U//~~FOUO~~) **Approved Safes** - The KG-189 is installed in an NSA-approved COMSEC container or a General Services Administration approved information processing container. (See NSTISSP No. 10.)

SECTION VII - (U) REPORTABLE COMSEC INCIDENTS

28. (U) **Reportable Incidents** - Listed below are COMSEC incidents associated with the KG-189 system that must be reported in accordance with NSTISSI No. 4003:

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

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

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

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

e. (U) Unauthorized KG-189 software changes.

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

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

h. (U//~~FOUO~~)

i. (U//~~FOUO~~)

j. (U//~~FOUO~~)

k. (U//~~FOUO~~)

l. (U//~~FOUO~~)

m. (U//~~FOUO~~)

n. (U//~~FOUO~~)

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

Encls:
ANNEX A - References
ANNEX B - Definitions
ANNEX C - Acronyms

ANNEX A - REFERENCES

(U) The following references are cited in this doctrine:

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

b. **FED-STD-1037C**, Telecommunications: Glossary of Telecommunication Terms, August 1996.

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

d. **NSTISSI No. 4001**, Controlled Cryptographic Items, July 1996.

e. **NTISSI No. 4002**, Classification Guide for COMSEC Information, 5 June 1986.

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

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

h. **NSTISSI No. 4005**, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997.

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

j. **NSTISSI No. 7000**, TEMPEST Countermeasures for Facilities, 20 June 1994.

k. **NSA pamphlet**, Protective Technologies Implementation Procedures for the KG-189 Holographic Tamper Indication Labels, June 1999.

l. **NSTISSP No. 10**, National Policy Governing Use of Approved Security Containers in Information Systems Security Applications, August 1999.

ANNEX B - DEFINITIONS

(U) One system-unique definition and several definitions extracted from NSTISSI No. 4009 and FED-STD-1037C are presented below for reader convenience:

a. **Accounting Legend Code** - Numeric code used to indicate the minimum accounting controls required for items of accountable COMSEC material within the COMSEC Material Control System. (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. **Controlling Authority** - Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet. (NSTISSI No. 4009)

d. **Cooperative Key Generation** - Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit. (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, filling, using, and destroying of electronic key and management of other types of COMSEC material. (NSTISSI No. 4009)

f. **FIREFLY** - Key management protocol based on public key cryptography. (NSTISSI No. 4009)

g. **Loop-Back** - 1. Method of performing transmission tests of access lines from the serving switching center, a method that usually does not require the assistance of personnel at the served terminal. 2. Method of testing between stations (not necessarily adjacent) wherein two lines are used, with the testing being done at one station and the two lines interconnected at the distant station. (FED-STD-1037C)

h. **Maintenance Key** - Key intended only for in-shop use. (NSTISSI No. 4009)

i. **Operational Key** - Key intended for use over-the-air for protection of operational information or for the production or secure electrical transmission of key streams. (NSTISSI No. 4009)

j. **Over-the-Air Rekeying (OTAR)** - Changing the traffic encryption key or transmission security key in remote crypto-equipment by sending new key directly to the remote crypto-equipment over the communications path it serves. (NSTISSI No. 4009)

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

l. **Short Title** - Identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling. (NSTISSI No. 4009)

m. **System High** - Highest security level supported by an information system. (NSTISSI No. 4009)

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

o. **Test Key** - Key intended for testing of COMSEC equipment or systems. (NSTISSI No. 4009)

p. **Traffic Flow Security** - Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system. (NSTISSI No. 4009)

q. **User Representative** - Person authorized by an organization to order COMSEC keying material and interface with the keying system: providing information to key users and ensuring the correct type of key is ordered. (NSTISSI No. 4009)

r. **Virtual Circuit** - A communications arrangement in which data from a source user may be passed to a destination user over various real circuit configurations.

NOTE: Virtual circuits are generally set up on a per-call basis and are disconnected when the call is terminated; however, a permanent virtual circuit can be established as an option to provided a dedicated link between two facilities. (FED-STD-1037C)

ANNEX C - ACRONYMS

Acronyms used in this doctrine are expanded below:

ALC - Accounting Legend Code

ASP - Accredited Security Parameter

CA - Controlling Authority

CCI - Controlled Cryptographic Item

CF - Central Facility

COMSEC - Communications Security

DODAAC - Department of Defense Activity Address Code

EKMS - Electronic Key Management System

INFOSEC - Information Systems Security

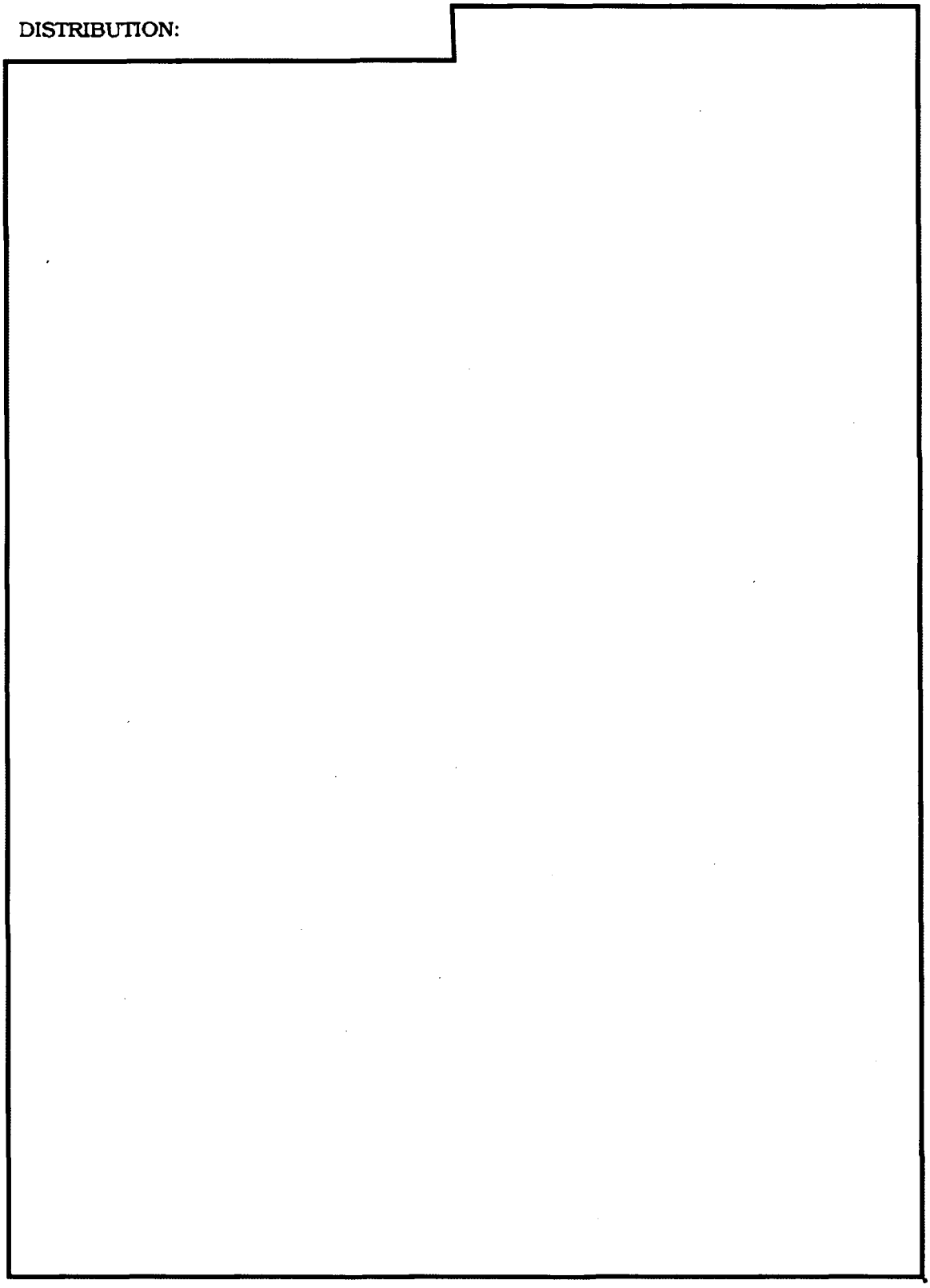
KSD - Key Storage Device

NSA - National Security Agency

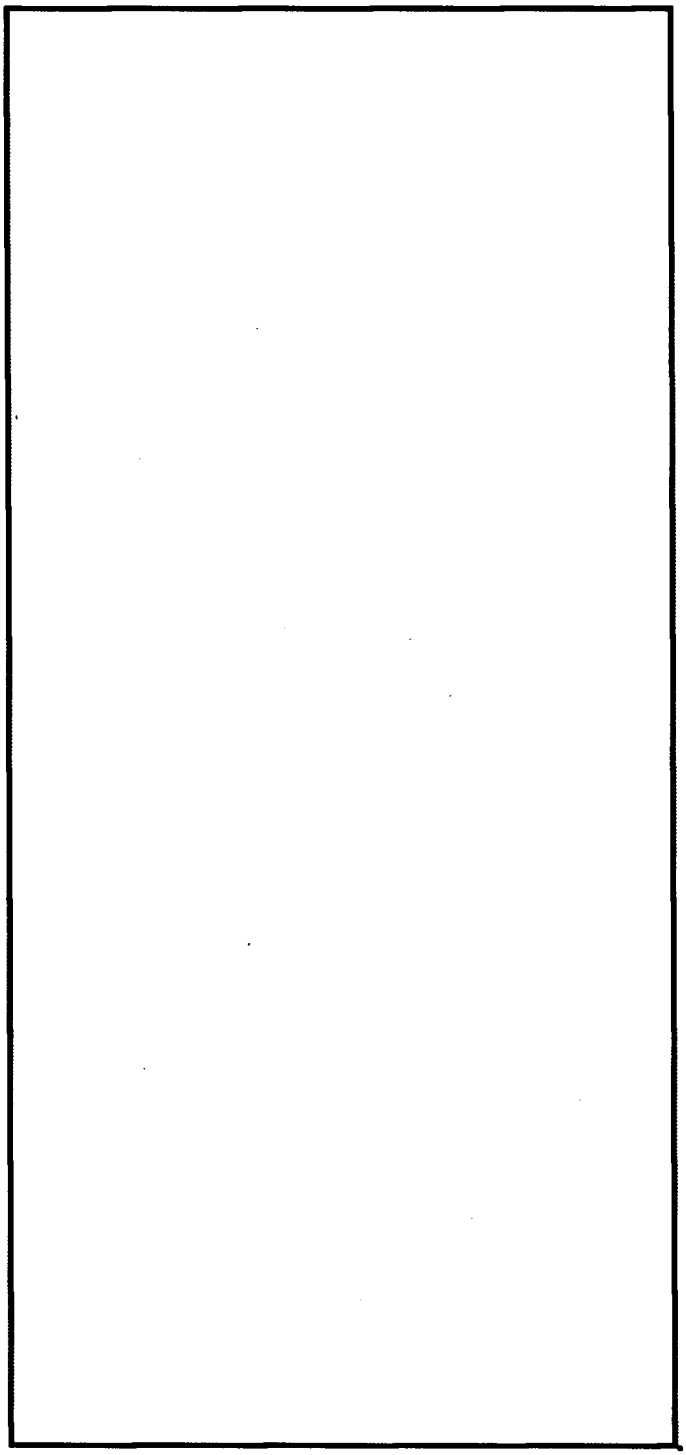
TEK - Traffic Encryption Key

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:



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



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