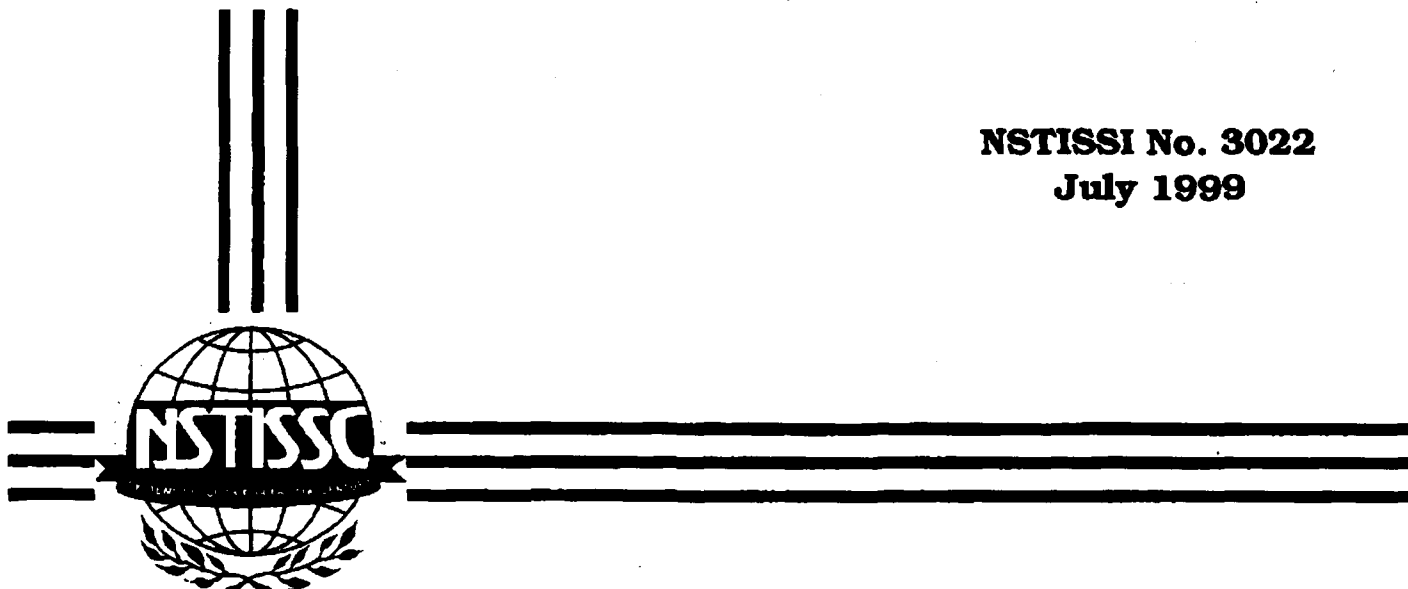


~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**NSTISSI No. 3022**

**July 1999**



~~(U//FOUO)~~ **OPERATIONAL SECURITY DOCTRINE**  
**FOR**  
**TRUNK ENCRYPTION DEVICES (TEDs)**  
**KG-81, KG-94 FAMILY, KG-95 FAMILY, KG-194**  
**FAMILY, AND KIV-19**  
**IN STAND-ALONE APPLICATIONS**

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

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



National Security Telecommunications And Information Systems Security Committee

## NATIONAL MANAGER

### FOREWORD

1. (U) This doctrine establishes the minimum national standards for safeguarding, controlling, and using TEDs and their associated COMSEC material in stand-alone (non-TRI-TAC) applications.

2. (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

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

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



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~(U//FOUO)~~ OPERATIONAL SECURITY DOCTRINE FOR TRUNK ENCRYPTION DEVICES  
(TEDs): KG-81, KG-94 FAMILY, KG-95 FAMILY, KG-194 FAMILY, AND KIV-19 IN STAND-ALONE APPLICATIONS

	SECTION
PURPOSE .....	I
APPLICABILITY AND SCOPE .....	II
EQUIPMENT DESCRIPTION .....	III
KEYING .....	IV
RESTRICTIONS .....	V
CLASSIFICATION/MARKING/ACCOUNTABILITY .....	VI
PHYSICAL SECURITY .....	VII
REPORTABLE COMSEC INSECURITIES .....	VIII

**SECTION I - (U) PURPOSE**

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

**SECTION II - APPLICABILITY AND SCOPE**

2. **(U) Applicability** - The provisions of this document apply to all departments and agencies of the U.S. Government and their contractors who use the specified TEDs.

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 TEDs. 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) National Security Agency. ATTN: Information Systems Security (INFOSEC) Policy and Doctrine Division.

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

6. **(U) Definitions** - Selected definitions from 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 shown.

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

1. (U) CCITT = Consultative Committee on International Telephone and Telegraph, which has been retitled "International Telecommunications Union - Telecommunications Sector" (ITU-T)

7. **(U) Document Supersession** - This document supersedes National Security Agency (NSA) letter doctrines, Serial S-0213-90, "Interim Operational Security Doctrine for the KG-95 Trunk Encryption Device (TED)," dated 21 November 1990, Serial S-0075-91 "Interim Operational Security Doctrine for the KG-95(E-1) Trunk Encryption Device (TED)," dated 30 May 1991, and Serial: X8-070-94 "Operational Security Doctrine for the Trunk Encryption Devices (TEDs): KG-81, KG-94 Family, KG-95 Family, and KG-194 Family in Stand Alone Applications," dated 7 June 1994.

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

a. **(U) Unkeyed Controlled Cryptographic Item (CCI)** - NSTISSI No. 4001 states the minimum requirements for safeguarding, controlling, and disposing of unkeyed CCIs, including the specified TEDs, 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 TOP SECRET key and keyed TED 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 TED trunks are terminated.

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

f. **(U) Potential Document Conflicts**

(1) **(U) Superior Authority** - Except as stated in the next paragraph, when the provisions of this instruction appear to substantially 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, NSTISS (see para 4.).

(2) **(U//FOUO)** [Redacted]

**SECTION III - (U) EQUIPMENT DESCRIPTION**

9. **(U) Capability** - The specified TEDs are on-line, full-duplex, COMSEC equipment used for the processing of serial, bulk traffic at high speeds. Within technical constraints as explained in maintenance manuals and equipment/systems documents, they can also be used in configurations other than full-duplex.

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

a. **(U//FOUO)** [Redacted]

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

NOTE: (U//FOUO)

[Redacted]

b. (U//FOUO)

[Redacted]

(1) (U//FOUO)

[Redacted]

(2) (U//FOUO)

[Redacted]

(3) (U//FOUO)

[Redacted]

(4) (U//FOUO)

[Redacted]

c. (U//FOUO)

[Redacted]

(1) (U//FOUO)

[Redacted]

(2) (U//FOUO)

[Redacted]

(3) (U//FOUO)

[Redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

[Redacted]

(4) (U//FOUO)

[Redacted]

d. (U//FOUO)

[Redacted]

10. (U) **Traffic Classification** - When appropriately keyed and configured, the specified TEDs are approved for the transmission of all categories and classifications of digital information.

11. (U) **Mounting Frames**

a. (U//FOUO)

[Redacted]

b. (U//FOUO)

[Redacted]

c. (U//FOUO)

[Redacted]

**SECTION IV - (U) KEYING**

12. (U) **Types of Key** - The following types of key are used in the TEDs:

a. (U//FOUO)

[Redacted]

b. (U//FOUO)

[Redacted]

c. (U) **Over-the-Air Test Key** - Over-the-air test key for the KG-81 and KG-94 Family equipment is AKZT-C5581 and for the KG-95 and KG-194 Family equipment is USKZT-C5582. Both keys are UNCLASSIFIED, are marked "CRYPTO," and are assigned ALC-1:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

d. (U) **Maintenance Key** is intended for bench testing. It is unclassified, is not marked "CRYPTO." and is assigned ALC-4, initial receipt required.

13. (U//FOUO)

[Redacted]

a. (U) **TEK Mode** - All of the specified TEDs can load and use TEKs.

b. (U//FOUO)

[Redacted]

14. (U//FOUO)

[Redacted]

a. (U//FOUO)

[Redacted]

b. (U//FOUO)

[Redacted]

c. (U//FOUO)

[Redacted]

15. (U) **Operational Configurations** - The covered TEDs may be used in a variety of operational configurations. The major configurations are:

a. (U//FOUO)

[Redacted]

b. (U//FOUO)

[Redacted]

c. (U//FOUO)

[Redacted]

d. (U//FOUO)

[Redacted]

e. (U//FOUO)

[Redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

16. (U) **Cryptographic Modes** - The specified TEDs are capable of operating in either of two cryptographic modes:

a. (U//~~FOUO~~) **Primary Mode** -

[Redacted]

b. (U) **Secondary Mode** - Use of the secondary mode to transmit classified information requires a waiver from the National Manager, NSTISS (see para 4).

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

[Redacted]

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

[Redacted]

18. (U) **Cryptoperiods**

a. (U) **TEK Cryptoperiods** - Authorized TED TEK cryptoperiods are:

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

[Redacted]

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

[Redacted]

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

[Redacted]

NOTE: (U) TEK in the "GC" format (1 copy each of 16 unique segments - monthly cryptoperiod) and annual canister supersession should be requisitioned for this application.

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

[Redacted]

NOTE: (U) TEK in the "VA" format (1 copy each of 62 unique segments - daily cryptoperiod) with bi-monthly canister supersession should be requisitioned for this application.



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(2) (U//FOUO)

[Redacted]

NOTE: (U) TEK in the "GC" format should be requisitioned for this application.

b. (U) FIREFLY Key

(1) (U//FOUO)

[Redacted]

NOTE: (U//FOUO)

NOTE: (U//FOUO)

(2) (U//FOUO)

NOTE: (U//FOUO)

c. (U) Cryptoperiod Extension - CAs may, without filing a COMSEC incident report, grant cryptoperiod extensions under the following conditions:

(1) (U//FOUO)

[Redacted]

(2) (U//FOUO)

d. (U) Cryptonet Size

(1) (U//FOUO)

[Redacted]

(2) (U//FOUO)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

19. (U//FOUO) [Redacted]

**SECTION V - (U) RESTRICTIONS**

20. (U//FOUO) [Redacted]

21. (U//FOUO) [Redacted]

22. (U//FOUO) [Redacted]

23. (U//FOUO) [Redacted]

**SECTION VI - (U) CLASSIFICATION/MARKING/ACCOUNTABILITY**

24. (U) **General Guidance** - NSTISSI No. 4002 provides general classification guidance for COMSEC information. The following guidance also applies:

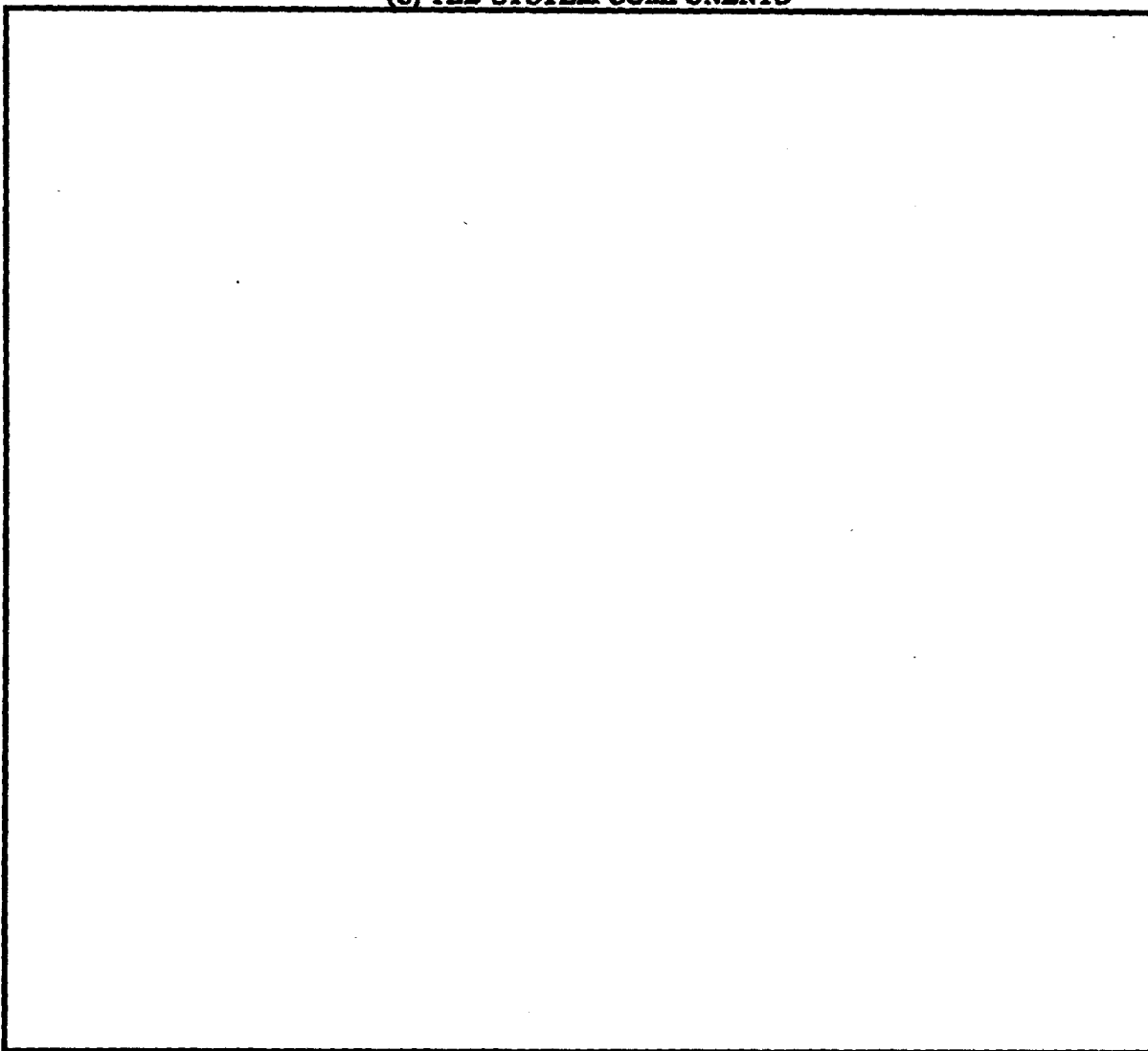
a. (U//FOUO) **TED System Components** [Redacted]

**(U) TED SYSTEM COMPONENTS**

[Redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**(U) TED SYSTEM COMPONENTS**



b. (U//FOUO)



c. (U//FOUO)



d. (U//FOUO)



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**SECTION VII - (U) PHYSICAL SECURITY**

25. **(U) Keyed Equipment** - When persons in a TED terminal area are not cleared to the level of the keyed equipment, TEDs must be under the operational control and within the view of at least one appropriately cleared person.

26. **(U) Installed Equipment and Terminal Spaces** - Installed TEDs and the terminal spaces in which they are located must be safeguarded in accordance with NSTISSI No. 4005. The operational status of any TED falls into one of the following groups:

a. **(U) Full-time Operated/Full-time Manned Trunks** - All persons authorized uncontrolled access to TED terminal areas must be cleared at least to the highest level of the information the TED-secured trunks are authorized to pass.

b. **(U//FOUO)**

**NOTE: (U//FOUO)**

c. **(U//FOUO)**

**NOTE: (U)** Although a responsible commander may prescribe additional security measures, the minimum requirement is that the doors to spaces in which TEDs are installed must be locked and effective controls be exercised over the door keys.

d. **(U) Unattended Terminal Facilities** - In addition to the requirements specified in paragraphs 28.b and 28.c above, TEDs may be operated at unattended sites, if the following conditions are met:

(1) **(U) Cryptonet Sizes** - Cryptonets for TEKs used with TEDs located at unattended sites must be kept as small as possible, with P-T-P key used where feasible.

(2) **(U//FOUO)**

(3) **(U) Storing Key** - Only that key that is electrically or physically held in the installed TEDs may be stored at unattended sites.

e. **(U) Installation** - TEDs must be installed in accordance with NSTISSAM TEMPEST/2-95, but deviations from these installation guidelines may be granted by responsible TEMPEST authorities.

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

f. (U) Safeguarding Installed Equipment and Terminal Spaces in SCIFs - TEDs installed in SCIFs must be safeguarded in accordance with the DCID 1/21.

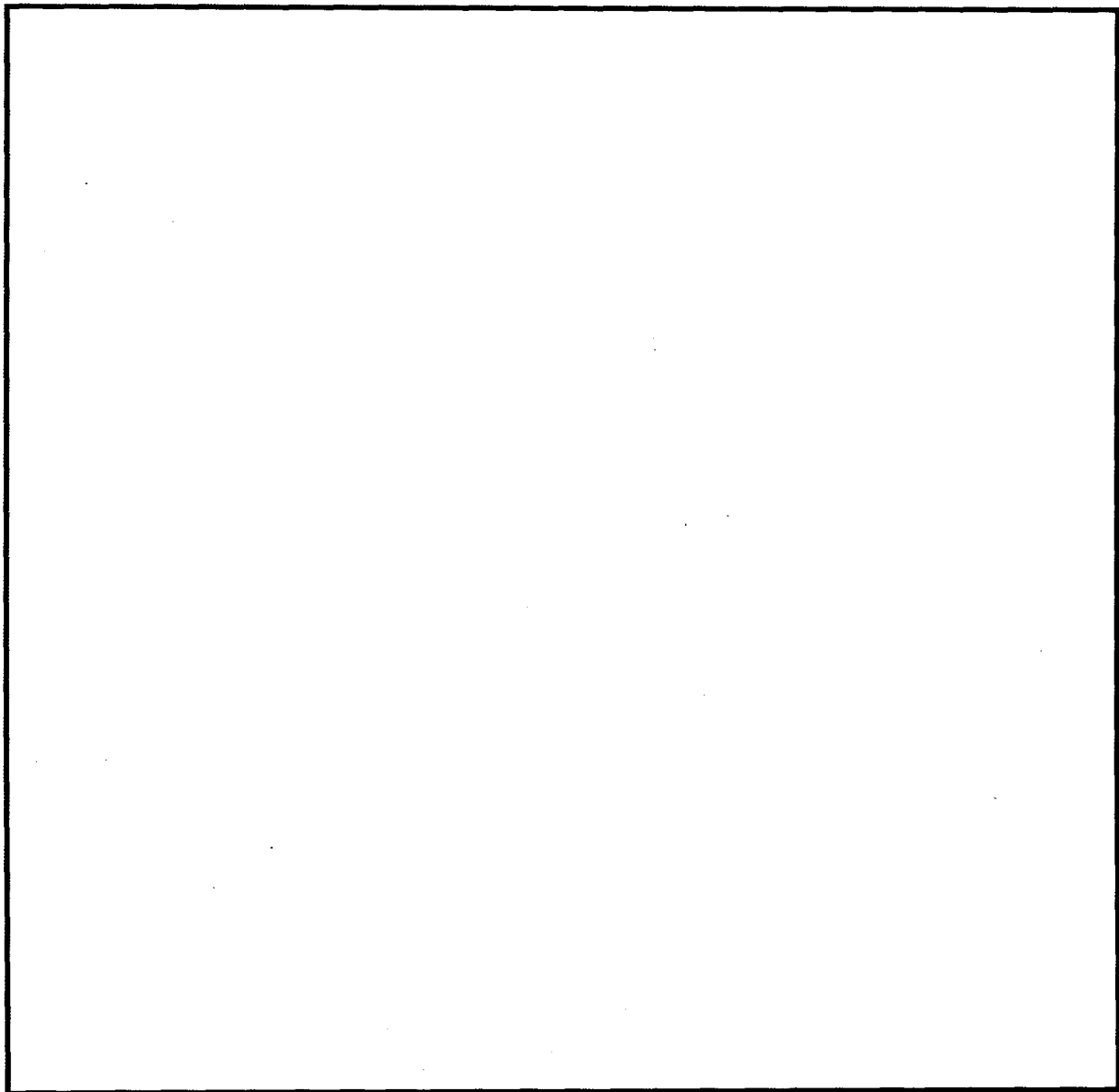
27. (U//FOUO)



28. (U//FOUO)



**(U) KSD-64A ZEROIZATION AND SHIPPING METHODS IN U.S. AND ITS TERRITORIES**



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**NOTE: (U)** The mandatory reuse program recognizes that depots and local COMSEC custodians/managers may have local requirements to reuse KSD-64A. Once properly zeroized, KSD-64As may be reused by their users or by a depot or the central facility. In addition, the central facility is authorized to provide zeroized or blank KSDs to users upon request.

**NOTE: (U//FOUO)**

**(U//FOUO)**

29. **(U//FOUO)**

**SECTION VIII - (U) REPORTABLE COMSEC INCIDENTS**

30. **(U)** NSTISSI No. 4003 contains a general listing of reportable COMSEC incidents and the standards for reporting them. Reportable incidents that are unique to the specified TEDs are listed below.

a. **(U//FOUO)**

b. **(U//FOUO)**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

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

c. (U) **Unauthorized Cryptoperiod** - Using a TED TEK beyond its authorized cryptoperiod.

d. (U//FOUO)

e. (U//FOUO)

f. (U//FOUO)

g. (U//FOUO)

h. (U//FOUO)

i. (U//FOUO)

j. (U//FOUO)

k. (U) **Retention of Effective Key Tape Segments** - Retaining effective segments of TED TEK for more than twelve hours after they are loaded into a COMSEC equipment.

Encls:

- ANNEX A, References
- ANNEX B, Definitions

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

**UNCLASSIFIED****(U) ANNEX A - REFERENCES**

The following documents are referenced in this doctrine. Reference to these documents is unclassified.

- a. **NSTISSI No. 4001**, "Controlled Cryptographic Items," dated July 1996.
- b. **NSTISSI No. 4004**, "Routine Destruction and Emergency Protection of COMSEC Material," dated 11 March 1987.
- c. **NSTISSI No. 4005**, "Safeguarding Communications Security (COMSEC) Facilities and Materials," dated August 1997.
- d. **NSTISSI No. 4006**, "Controlling Authorities for COMSEC Material," dated 2 December 1991.
- e. **NSTISSD No. 502**, "National Security Telecommunications and Automated Information Systems Security," dated 5 February 1993.
- f. **NSTISSI No. 4009**, "National Information Systems Security (INFOSEC) Glossary," dated August 1997.
- g. **FED STD 1037C**, General Services Administration, "Telecommunications: Glossary of Telecommunication Terms," dated August 16, 1996.
- h. **NSTISSI No. 4002**, "Classification Guide for COMSEC Information," dated 5 June 1986.
- i. **NSTISSI No. 3021**, "Operational Security Doctrine for the AN/CYZ-10/10A," dated September 1997.
- j. **NSTISSAM TEMPEST/2-95**, "RED/BLACK Installation Guidelines," dated 12 December 95.
- k. **DCID 1/21**, Director of Central Intelligence, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," dated 29 July 1994.
- l. **NSTISSI No. 4003**, "Reporting and Evaluating COMSEC Incidents," dated 2 December 1991.



**UNCLASSIFIED****(U) ANNEX B - DEFINITIONS**

Selected definitions from NSTISSI No. 4009 and FED STD 1037C are quoted below for reader convenience. Other applicable definitions unique to this NSTISSI are also quoted. The following definitions are UNCLASSIFIED in their entirety.

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. **BLACK** - Designation applied to information systems and to associated areas, circuits, components, and equipment in which national security information is not processed. (NSTISSI No. 4009)

c. **Bulk Encryption** - Simultaneous encryption of all channels of a multilateral telecommunications trunk. (FED STD 1037C & NSTISSI No. 4009)

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

e. **FIREFLY Key** - Electronic key that allows KG-95 and KG-194 family equipment to generate per call key. (NSTISSI No. 3022 unique)

f. **Full-time Operated/Full-time Manned Trunk** - TED-secured trunk that operates continuously, with both terminals located in areas that are continuously manned by appropriately cleared personnel. (NSTISSI No. 3022 unique)

g. **Full-time Operated/Part-time Manned Trunk** - TED-secured trunk that operates continuously but has one or both of its terminals located in a space that is not continuously manned by appropriately cleared personnel. (NSTISSI No. 3022 unique)

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

**NOTE:** "Key" has replaced the terms "variable," "keying variable," and "cryptovisible."

i. **Loop-back** - Method of performing transmission tests of access lines from the serving switching center, which usually does not require the assistance of personnel at the served terminal. Two lines are used, with the testing being done at one station and with the two lines interconnected at the distant station. (FED STD 1037C)

j. **Network** - 1. An interconnection of three or more communicating entities and (usually) one or more nodes. 2. A combination of passive or active electronic components that serves a given purpose. (FED STD 1037C)

k. **Node** - A terminal of any branch of a network or an interconnection common to two or more branches of a network. (FED STD 1037C)

**B-1**  
**UNCLASSIFIED**

ANNEX B to  
NSTISSI No. 3022

**UNCLASSIFIED**

l. **Part-time Operated/Part-time Manned Trunk**. TED-secured trunk that operates only when both terminals are manned by appropriately cleared personnel. (NSTISSI No. 3022 unique)

m. **Primary Mode of Operation** - The normal cryptographic mode for operation of TEDs. (NSTISSI No. 3022 unique)

n. **Secondary Mode of Operation** - An alternate cryptographic mode of operation for TEDs that can be used under certain conditions. (NSTISSI No. 3022 unique)

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

p. **Sensitive Information** - Any information, the loss or 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 section 552a, title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (NSTISSI No. 4009)

**NOTE:** Since the Computer Security Act of 1987 applies only to unclassified information that deserves protection, "sensitive information" is inherently "sensitive unclassified information."

q. **Trunk** - A single transmission channel between two points that are switching centers or nodes or both. (FED STD 1037C)

r. **Unattended Terminal** - TED-secured trunk terminal area in which no appropriately cleared personnel are present. (NSTISSI No. 3022 unique)

Doc Ref ID: A309754  
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

---