

NSTISSI No. 3020

11 February 1992

NSTISS

NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR THE

KL-51 (RACE)

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

~~**FOR OFFICIAL USE ONLY**~~

NSTISS
NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS SECURITY**NATIONAL MANAGER**

11 February 1992

FOREWORD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3020 provides minimum security doctrine for the operational use of the KL-51 (RACE) equipment and associated COMSEC material.

2. Extracts from this document may be made as necessary. Extracts must be marked FOR OFFICIAL USE ONLY, and cannot be given to the public without the specific approval of the National Manager, NSTISS.

3. The responsibility for distributing and implementing this instruction to subordinate elements rests with the Chiefs of the Military Services and heads of federal departments and agencies.

4. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction from:

Executive Secretariat
National Security Telecommunications and
Information Systems Security Committee
National Security Agency
Ft. George G. Meade, MD 20755-6000

5. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.



W. O. STUEDEMAN
Vice Admiral, U.S. Navy

~~FOR OFFICIAL USE ONLY~~

**OPERATIONAL SECURITY DOCTRINE
FOR THE KL-51 (RACE)**

<u>TITLE</u>	<u>SECTION</u>
PURPOSE AND SCOPE.....	I
EXCEPTIONS.....	II
REFERENCES.....	III
DEFINITIONS.....	IV
SYSTEMS DESCRIPTION.....	V
KEYING.....	VI
CLASSIFICATION GUIDANCE.....	VII
PHYSICAL SECURITY.....	VIII
DESTRUCTION AND EMERGENCY PROTECTION.....	IX
REPORTABLE INCIDENTS.....	X

SECTION I - PURPOSE AND SCOPE

1. This document provides minimum security doctrine for the operational use of the KL-51 (RACE) and associated COMSEC material. The KL-51 is a portable off-line encryption device which was developed by the Norwegians for NATO use and was called "RACE," and was subsequently adopted to satisfy U.S. national off-line needs. This document will be made available to all U.S. Government organizations that use or have access to the KL-51 and related COMSEC material. Promulgation may be made through issuance of this document or through its incorporation into applicable Service, department, or agency publications.

SECTION II - EXCEPTIONS

2. Requests for exceptions to any of the provisions of this NSTISSI must be submitted to DIRNSA (ATTN:) , for approval prior to implementation. All requests for exceptions must be accompanied by complete operational justification.

SECTION III - REFERENCES

3. **Reference Listing.**

a. NACSI No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.

NSTISSI No. 3020

- b. NCSC-9, National COMSEC Glossary, dated 1 September 1982.
- c. KAO-196, Guidelines for the use and Operation of the TSEC/KL-51, dated June 1983.
- d. NTISSI No. 4002, Classification Guide for COMSEC Information, dated 5 June 1986.
- e. AMSG-293, NATO Cryptographic Instructions, dated January 1987.
- f. NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.
- g. NTISSI No. 4005, Control of TOP SECRET Keying Material, dated 17 July 1987.
- h. NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, dated 1 February 1991.
- i. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991.
- j. NSTISSI No. 4006, Controlling Authorities for COMSEC material, dated 2 December 1991.

SECTION IV - DEFINITIONS

4. The definitions in the National COMSEC Glossary (NCSC-9) apply. Additional definitions follow:

a. **Key.** Information (usually a sequence of random or pseudorandom binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or producing other keys.

NOTE: "Key" replaces the terms "variable," "key variable," and "cryptovisible."

b. **Traffic Encryption Key (TEK).** Key used to encrypt plain text or to superencrypt previously encrypted text, and/or to decrypt cipher text.

NSTISSI No. 3020

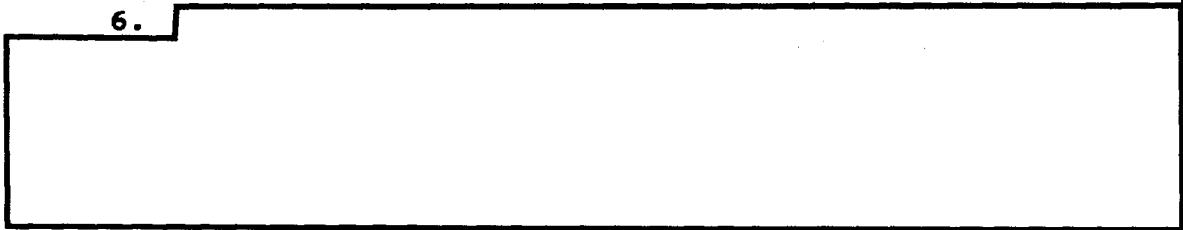
c. System Indicator. A symbol or group of symbols in an off-line encrypted message which identifies the specific cryptosystem or key used in the encryption.

d. Two-Person Integrity (TPI). A system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures, with respect to the task being performed (e.g., TOP SECRET keys).

NOTE: The concept of "Two-person integrity" procedures differs from "no-lone zone" procedures in that under TPI controls, two authorized persons must directly participate in the handling and safeguarding of the keying material (as in accessing storage containers, transportation, keying/rekeying operations, and destruction). No-lone zone controls are less restrictive in that the two authorized persons need only to be physically present in the common area where the material is located. Two-person control refers to nuclear command and control material while two-person integrity refers only to COMSEC keying material.

SECTION V - SYSTEM DESCRIPTION

5. The KL-51 is a portable, off-line, CONFIDENTIAL COMSEC equipment designed for encryption/decryption of alphanumeric information. It has two built-in means for input, a keyboard and a tape reader, and a built-in, light-emitting diode (LED) display for readout of input/output information; the KL-51 can also receive input from a peripheral keyboard. In addition, the KL-51 may be connected to a teleprinter and/or a tape punch, but in an off-line mode only. The teleprinter interface allows both input and output, while the tape punch interface is only for output from the KL-51. The KL-51 shall not be connected to other line-connected or on-line peripheral equipment without prior approval of the National Manager. The KL-51 may be set up in tactical environments, or installed in fixed locations.

6. 

NSTISSI No. 3020

7. [Redacted]

8. [Redacted]

SECTION VI - KEYING

9. **Controlling Authority.** Controlling authority responsibilities for the KL-51 key shall be in accordance with NSTISSI No. 4006.

10. **Key Format.** KL-51 keying material is produced in punched tape form as maintenance or training key packaged in resealable plastic boxes, or as operational, exercise, or test key packaged in protective canisters. The packaging, marking, safeguarding, and control of all key tapes classified up to and including TOP SECRET, marked "CRYPTO," shall be in accordance with NACSI No. 4005 and NTISSI No. 4005.

a. Operational, exercise, or test key is used when KL-51 encrypted messages will be transmitted (electrically or physically). There are two types of this key: traffic encryption key (TEK) and system indicator key (SIK).

(1) TEKs are used to encrypt/decrypt messages and they may be loaded into the KL-51 in the first 25 (A to Y) key storage locations. These key storage locations allow participation in up to 25 different cryptonets or may be used by mobile/tactical users to store future key. Each NATO TEK canister contains 62 TEK segments, using the "VA" format. Each U.S. TEK canister contains 31 TEK segments, using the "AA" format.

(2) SIKs are used to encrypt/decrypt system indicators; they are loaded into the KL-51 in the 26th (Z) key storage location only. Each SIK canister contains 30 SIK segments (six unique SIKs, five copies each), using the "DC" format. Multiple copies of SIKs are included to accommodate:

(a) The need to reload a SIK, especially where the KL-51 is not in continuous operation.

NSTISSI No. 3020

(b) The use of identical SIKs from one canister to load several pieces of equipment.

b. Maintenance and classroom training key are not marked "CRYPTO." Maintenance key is used only for bench testing and repair of KL-51 equipment and not for over-the-air transmissions. Training key is used only for classroom type training and not for over-the-air transmissions.

11. Classification of Key.

a. TEKs are classified to the highest level of the traffic they are intended to protect, marked "CRYPTO," and assigned ALC-1.

b. There are two types of SIKs; both are marked "CRYPTO" and are classified to the highest level of the traffic they are intended to protect or at a minimum of CONFIDENTIAL, and assigned ALC-1. The two types of SIKs facilitate inter-operability, and are assigned the following applications:

(1) AMST - for NATO use. Access will be in accordance with AMSG-293.

(2) USKAT - for U.S. use. Access will be in accordance with NACSI No. 4005.

c. Maintenance and classroom training keys are UNCLASSIFIED, marked FOUO (FOR OFFICIAL USE ONLY), and assigned ALC-4.

12. Cryptoperiods.

a. KL-51 TEKs have a 24-hour cryptoperiod; each 62-segment NATO TEK canister is superseded every two months, and each 31-segment U.S. TEK canister is superseded monthly. When operational requirements necessitate, controlling authorities may extend the cryptoperiod by one week.

b. KL-51 SIKs have a one-month cryptoperiod and each 30-segment SIK canister is superseded after six months. Normally, a used SIK tape segment is destroyed immediately after successful keying of equipment. If the last copy of key is the only copy available, it may be retained up to one week after its supersession for use in decryption of delayed messages. A segment so retained shall be protected sufficiently to preclude compromise through loss or subversion. At minimum, the classification shall be CONFIDENTIAL.

NSTISSI No. 3020

c. KL-51 maintenance and training key segments may be reused until unusable.

13. Cryptonet Limitations. Cryptonet sizes shall be kept as small as is operationally feasible. As the number of copies of a key grows, the vulnerability of that key to compromise increases, and compromise of key at one terminal potentially compromises the traffic of all users of that key.

14. Key Control. Key control must be performed in accordance with NTISSI No. 4004 and NACSI No. 4005. In addition, during travel away from controlled areas and where appropriate storage facilities are not available, the key must be protected in the personal custody of the user.

15. Ordering Key. Keying material must be ordered from NSA at least 120 days prior to use to ensure timely delivery of the key. Operational users must inform NSA when follow-on or replacement key is required. Without such notification, key will not be shipped, resulting in the user running out of key and necessitating emergency extensions and resupply. Military users should order their key through their Cryptologic Support Element.

SECTION VII - CLASSIFICATION GUIDANCE

16. Classification and Marking. For general COMSEC classification guidelines, see NTISSI No. 4002. Classifications and markings assigned to the KL-51 and its associated COMSEC material are listed in the annex to this document. Accounting Legend Codes (ALC) for these items represent the minimum accounting controls required.

SECTION VIII - PHYSICAL SECURITY

17. Physical Security. KL-51 equipment and associated COMSEC material are controlled in accordance with the general provisions of NACSI No. 4005. The KL-51 shall be protected commensurate with the classification of the key or the equipment (CONFIDENTIAL), whichever is higher. Additional requirements specific to the KL-51 system follow:

a. Program CHECK. CHECK is a self-diagnostic test procedure integral to the KL-51. Instructions for its use are included in the operating instructions for the KL-51

NSTISSI No. 3020

(KAO-196A). Since CHECK zeroizes all keys, including the SIK, it shall be performed at the end of each SIK cryptoperiod.

b.

(1)

(a)

(b)

(c)

(d)

(2)

(a)

(b)

(c)

(3)

c.

d. Maintenance and Maintenance Training. Maintenance and maintenance training guidelines are provided in NSTISSI No. 4000.

SECTION IX - DESTRUCTION AND EMERGENCY PROTECTION

18. Procedures for the destruction and emergency protection of the KL-51 equipment and associated COMSEC

NSTISSI No. 3020

material are in accordance with the general provisions of NTISSI No. 4004. It is understood that KL-51 devices may be used in various situations with only one person control. Under these circumstances, key tapes may be destroyed without a witness-for-destruction signature on the user/destruction cards (disposition record). This does not constitute a security violation or require an incident report. This scenario may be followed as an operational necessity or in emergency situations and not as a user convenience. Superseded KL-51 key may be retained up to one week to decrypt delayed messages. After the one-week retention time elapses, destruction of the key must be conducted by the user within 12 hours. Retention of used KL-51 keys longer than the one-week period must be approved on a case-by-case basis by the DIRNSA (ATTN:).

SECTION X - REPORTABLE INCIDENTS

19. Reportable incidents in general are addressed in NTISSI No. 4003. COMSEC incidents are reportable to DIRNSA (ATTN:). Incidents specific to the KL-51 follow:

a. Use of the KL-51 connected to on-line or line-connected peripheral equipment, other than described in paragraph 5. above, without prior approval of DIRNSA (ATTN:).

b. Missing or broken wire seals from the sealing screws on the KL-51 chassis upon initial receipt directly from the manufacturer. The wire seals serve the purpose of providing security during initial shipment from the manufacturer; they are removed after receipt of equipment to allow equipment check, and need not be replaced or reported missing thereafter.

Encl:

Annex - Classification Guidance for the KL-51

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

ANNEX**CLASSIFICATION GUIDANCE FOR THE KL-51**

<u>ITEM</u>	<u>CLASSIFICATION</u>	<u>ALC</u>
KL-51	Unkeyed - CONFIDENTIAL	1
	Keyed - Same classification as the key or the equipment (CONFIDENTIAL) whichever is higher.	
KAM-438A, Limited Maintenance Manual, KL-51	CONFIDENTIAL	1
KAM-439A, Full Maintenance Manual, KL-51	CONFIDENTIAL	1
KAO-196A, Operating Instructions, KL-51	CONFIDENTIAL	1

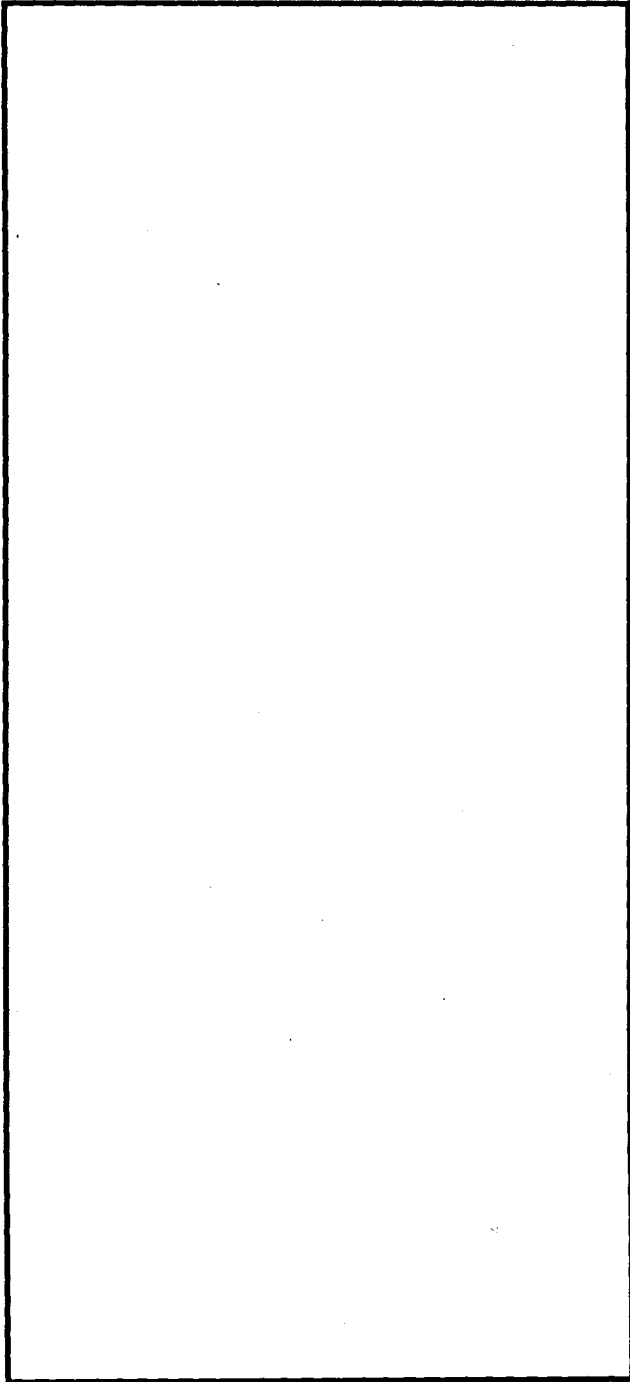
ANNEX to
NSTISSI No. 3020

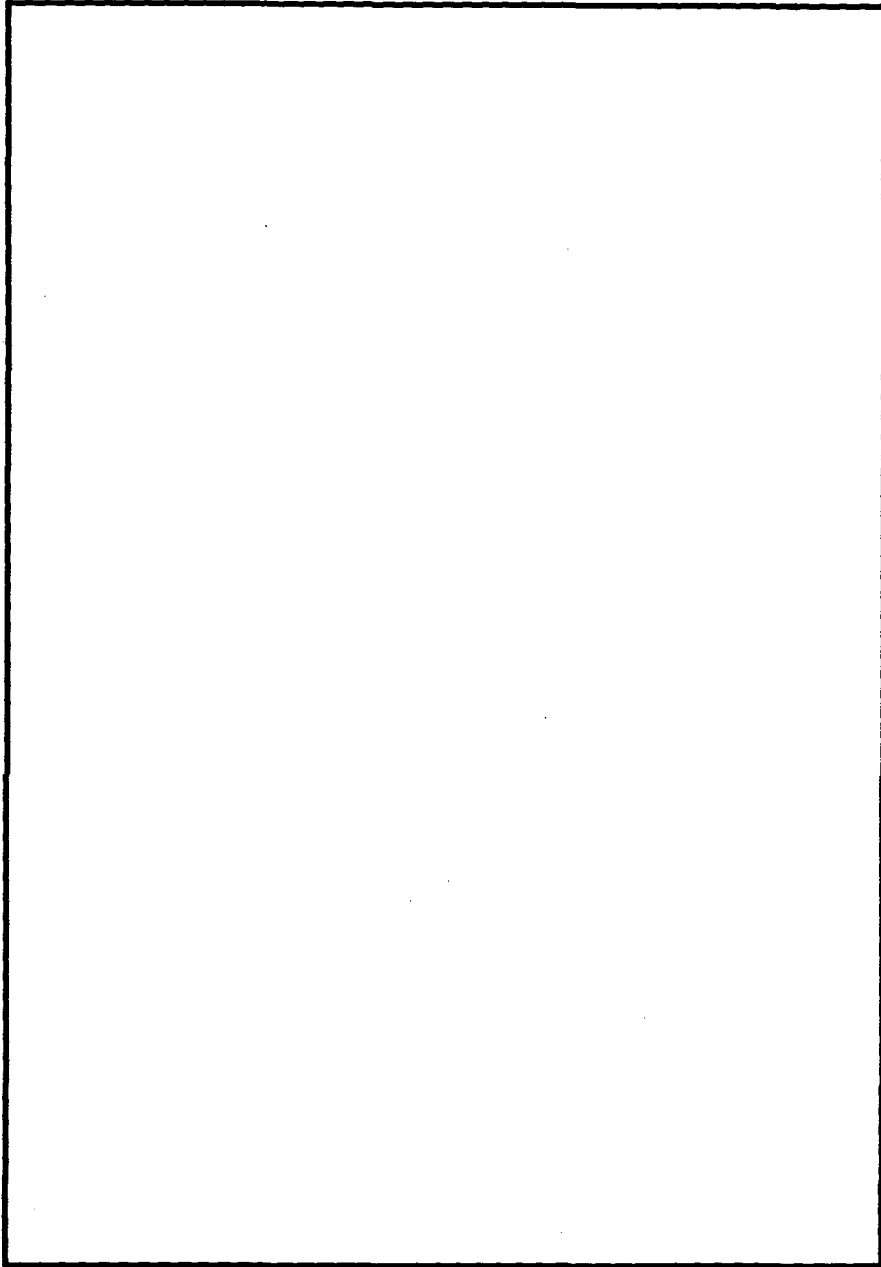
~~FOR OFFICIAL USE ONLY~~

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

NSTISSI No. 3020

DISTRIBUTION:
NSA





FOR OFFICIAL USE ONLY