

NTISSI 3002

DATE: 5 September 1986



NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

OPERATIONAL DOCTRINE

FOR THE KGV-9

REMOVABLE KEY STREAM GENERATOR MODULE

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

~~FOR OFFICIAL USE ONLY~~

NTAISS

NATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY

NATIONAL MANAGER

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

FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 3002, "Operational Doctrine for the KGV-9 Removable Key Stream Generator Module," establishes minimum standards for the safeguarding and control of the KGV-9 and keying material. Requests for waivers to any of the provisions of this NTISSI must be submitted to Director, National Security Agency, ATTN: [redacted], for approval prior to implementation.

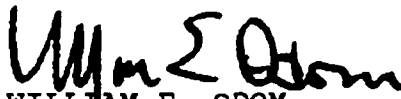
2. Additional copies of this Instruction may be obtained from:

Executive Secretariat
National Telecommunications and Information Systems
Security Committee
National Security Agency
Operations Building No. 3
Fort George G. Meade, MD 20755-6000

3. Extracts of information in this Instruction may be made as necessary. Such extracts shall be marked "FOR OFFICIAL USE ONLY," and shall not be made available to the general public without the specific approval of the National Manager, NTAISS.

4. Federal departments and agencies shall implement this Instruction within 120 days of the effective date. It is requested that one copy of each department or agency implementing directive be forwarded to the National Manager, ATTN: [redacted]

[redacted] National Security Agency, Fort George G. Meade, MD 20755-6000.



WILLIAM E. ODOM
Lieutenant General, USA

OPERATIONAL DOCTRINE FOR THE KGV-9
REMOVABLE KEY STREAM GENERATOR MODULE

SECTION

PURPOSEI
SCOPEII
REFERENCESIII
DEFINITIONSIV
CLASSIFICATION GUIDANCEV
EQUIPMENT DESCRIPTIONVI
KEYINGVII
PHYSICAL SECURITYVIII
DESTRUCTION AND EMERGENCY PROTECTIONIX
REPORTABLE INSECURITIESX

SECTION I - PURPOSE

1. This document prescribes general COMSEC doctrine for the operational use of the KGV-9 and related COMSEC material.

SECTION II - SCOPE

2. The provisions of this document apply to all departments and agencies of the U.S. Government and their contractors, who handle, distribute, account for, store, or use the KGV-9 and associated COMSEC material.

SECTION III - REFERENCES

3. References.

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

b. NACSI No. 4010, "Routine Destruction and Emergency Protection of COMSEC Material," dated 23 February 1982.

c. NACSI No. 4004, "Controlling Authorities for COMSEC Keying Material," dated 23 June 1982.

d. NCSC-9, "National COMSEC Glossary," dated 1 September 1982.

NTISSI No. 3002

e. NACSI No. 4008, "Safeguarding COMSEC Facilities," dated 4 March 1983.

f. NACSI No. 4006, "Reporting COMSEC Insecurities," dated 20 October 1983.

g. NTISSI No. 4001, "Controlled Cryptographic Items," dated 25 March 1985.

h. NTISSI No. 4002, "Classification Guide for COMSEC Information," dated 5 June 1986.

SECTION IV - DEFINITIONS

4. For purposes of this doctrine, the definitions in NCSC-9 apply, with the exception of the following terms which will be reflected in a future revision to NCSC-9:

a. Key - Information (usually a sequence of random binary digits) used to initially set up and to periodically change the operations performed in a crypto-equipment for purposes of encrypting or decrypting electronic signals; for determining electronic counter countermeasures (ECCM) patterns (e.g., frequency hopping or spread spectrum); or for producing other keys. ("Key" replaces the terms "variable," "key(ing) variable," and "cryptovisible.")

b. Key Stream - A sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem, to combine with plain text to produce cipher text, to control TRANSEC processes, or to produce other keys.

c. Transmission Security (TRANSEC) Key - A key that is used in the control of transmission security processes (e.g., frequency hopping and spread spectrum).

SECTION V - CLASSIFICATION GUIDANCE

5. General COMSEC classification guidance may be found in NTISSI No. 4002. Additional guidance follows:

a. The fact that the KGV-9 converts an externally generated input linear sequence into a cryptographically secure pseudorandom output sequence is UNCLASSIFIED. Reference to specific systems utilizing electronic counter countermeasures (ECCM), with reference to the cryptographic functions of the KGV-9, is also unclassified.

NTISSI No. 3002

b. Reports - Technical, operational, and project reports dealing with the KGV-9 must be classified by their originators on the basis of content. In general, information revealing cryptographic details of the KGV-9 must be classified SECRET in accordance with NTISSI No. 4002. Information concerning any vulnerabilities (cryptanalytic, TEMPEST, system, etc.) of the KGV-9 must be classified at least SECRET and be marked "Not Releasable to Foreign Nationals." COMSEC reports of all types are not releasable to the Defense Documentation Center.

c. Equipments, Ancillaries, Components, and Supporting Documentation:

| <u>ITEM</u> | <u>ACCOUNTA-</u> <u>BILITY</u> | <u>CLASSIFICATION/</u> <u>MARKING</u> | <u>CLEARANCE FOR ACCESS</u> | |
|--|--------------------------------------|--|------------------------------|--|
| | | | <u>UNKEYED</u> | <u>KEYED</u> |
| KGV-9 Production Models | By quantity | UNCLASSIFIED CCI | Clearance not required | Same as highest classification of key it con- tains |
| KAM-474A Maintenance Manual for KGV-9 | Accounting Legend Code (ALC)-1 | SECRET NOFORN | N/A | N/A |
| KYK-13 Electronic Transfer Device | By quantity | UNCLASSIFIED CCI | Clearance not required | Same as highest classification of key it contains |
| KOI-18 General Pur- pose Tape Reader | By quantity | UNCLASSIFIED CCI | Clearance not required | Does not store keys |

d. Unclassified diagrams and drawings of internal views of the KGV-9 must be marked "FOR OFFICIAL USE ONLY."

e. Information - No information concerning the operation, use, engineering data, or design detail of the KGV-9 may be released in the public domain without prior approval of the Director, National Security Agency (NSA).

SECTION VI - EQUIPMENT DESCRIPTION

6. The KGV-9 is a small, lightweight (3 pounds), high-speed (10 Mbps) key stream generator module which converts an externally generated input linear sequence into a cryptographically secure

NTISSI No. 3002

pseudorandom output sequence. It is intended for use within a host equipment and depends upon the host for generation of input signals, processing of output signals, and providing the physical and environmental interface necessary for proper operation. The KGV-9 provides transmission security and will be used in a number of spread spectrum anti-jam modems. The KGV-9 equipment will be operational in ground mobile, airborne, shipboard, and fixed-plant locations.

7.

SECTION VII - KEYING

8. Types of Keys. The KGV-9 uses two-part TRANSEC keys which are produced in punched paper tape form and are accompanied by specific handling/disposition instructions.

a. Operational, exercise, and test keys are packaged in protective plastic canisters, marked CRYPTO, and classified a minimum of CONFIDENTIAL. Each canister, which is superseded on an annual basis, contains 14 unique monthly segments copied three times each. The two additional monthly segments have been provided for back-up material in case of extended power failure to the modem or the KGV-9 during the cryptoperiod. (During initial set-up, unlimited equipment restarts are permitted.)

b. Maintenance keys, which are used for back-to-back (bench testing) maintenance purposes, are UNCLASSIFIED and are packaged in plastic pill boxes. These keys may be used indefinitely.

9. KGV-9 Key Loading. The KGV-9 keying (two segments) will be accomplished via the host equipment load connector using either a KOI-18 tape reader or a KYK-13 electronic transfer device.

10. Destruction of Key. After the two-part key has been successfully loaded into the KGV-9 and the entire cryptonet is successfully keyed and operational, the used tape segment must be destroyed. However, if all of the unique segments have been used down to the last copy of the last segment prior to the end of its cryptoperiod, that last segment may be retained for the duration of the cryptoperiod to facilitate any further required use. It should be noted that this segment must be carefully protected to preclude unauthorized access since it will not be in the protective canister. If the KYK-13 is used to load the KGV-9, then the

NTISSI No. 3002

KYK-13 storage registers containing the KGV-9 key must also be zeroized after successful loading.

11. Cryptoperiod. The cryptoperiod for KGV-9 TRANSEC keys is monthly. A 24-hour emergency cryptoperiod extension may be granted by the controlling authority in accordance with NACSI No. 4004. A key change should be initiated by the controlling authority when a known or suspected cryptographic failure or compromise occurs. In an emergency, when another key is not available, the same key may be used with the understanding that A/J protection provided by the KGV-9 while using that key can be lost if the enemy has recovered the key.

12. Cryptonet Size. A cryptonet is defined to include all links (KGV-9s) within one satellite area which hold the same key. Although a specific cryptonet size limitation is not prescribed, the general rule is that KGV-9 cryptonets should be kept as small as operationally feasible. The need for a common key to provide TRANSEC functions in a given network is recognized. However, users should understand that as the number of copies of a key increases and the key becomes more widely distributed, the vulnerability of that key to loss or unauthorized access also increases. In addition, large cryptonets inhibit the timely supersession of keying material in the event of a compromise.

SECTION VIII - PHYSICAL SECURITY

13. Production models of the KGV-9 are unclassified and designated Controlled Cryptographic Items (CCIs). As such, they must be protected in a manner at least equal to that which is normally provided to other high-value/sensitive material.

a. When keyed, the KGV-9 must be safeguarded in accordance with the classification of the keys it contains, as prescribed by NACSI No. 4005.

b. An unkeyed KGV-9 must be safeguarded as required by NTISSI No. 4001.

14. COMSEC Equipment Viewing. No restriction other than a valid "need-to-know" is imposed upon external viewing or other exposure to the KGV-9 where no opportunity for use, tampering, viewing of keys, or internal examination exists. However, the KGV-9 may not be displayed in public forums without NSA approval.

NTISSI No. 3002

SECTION IX - DESTRUCTION AND EMERGENCY PROTECTION

15. The requirements for the secure destruction of COMSEC material and for its safeguarding under emergency conditions are contained in NACSI No. 4010.

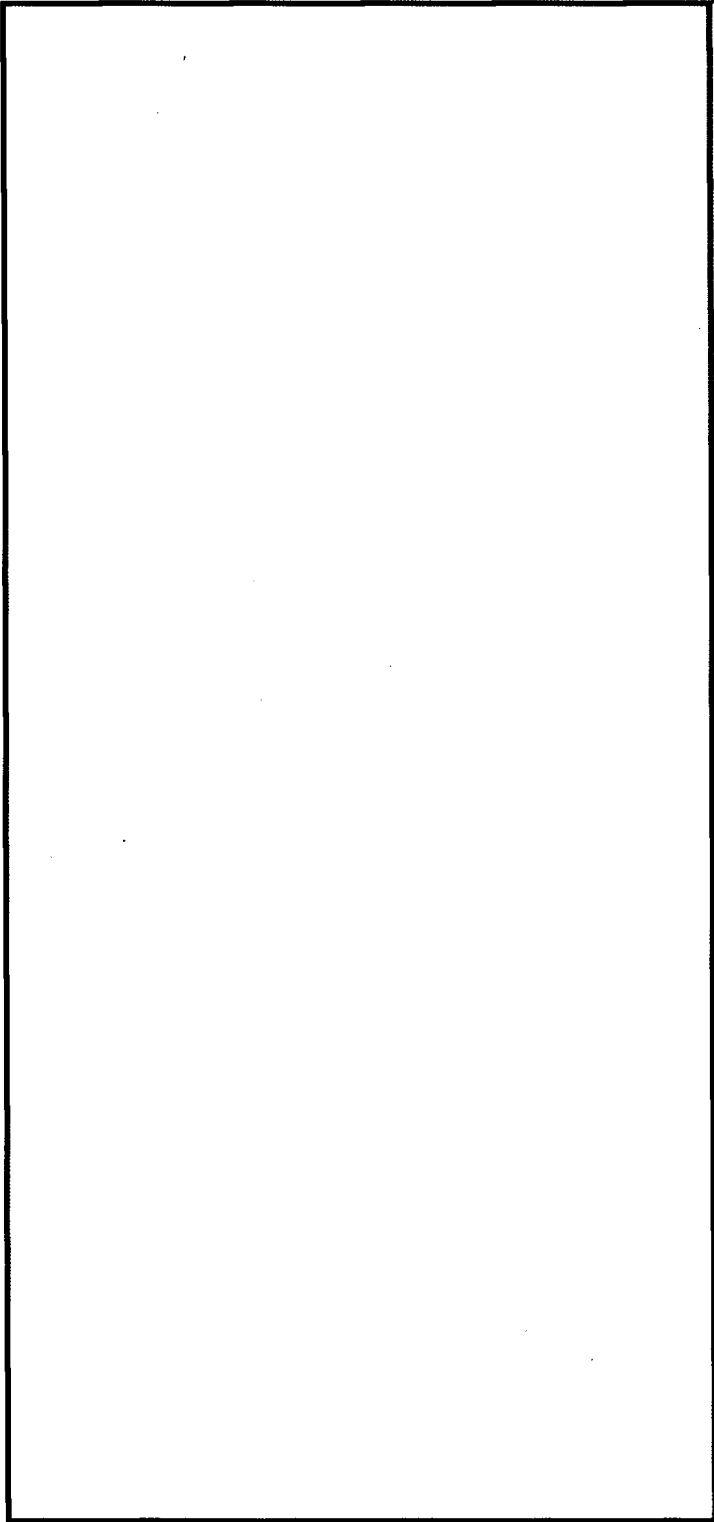
SECTION X - REPORTABLE INSECURITIES

16. Insecurities involving the KGV-9 and related COMSEC material are reportable in accordance with NACSI No. 4006.

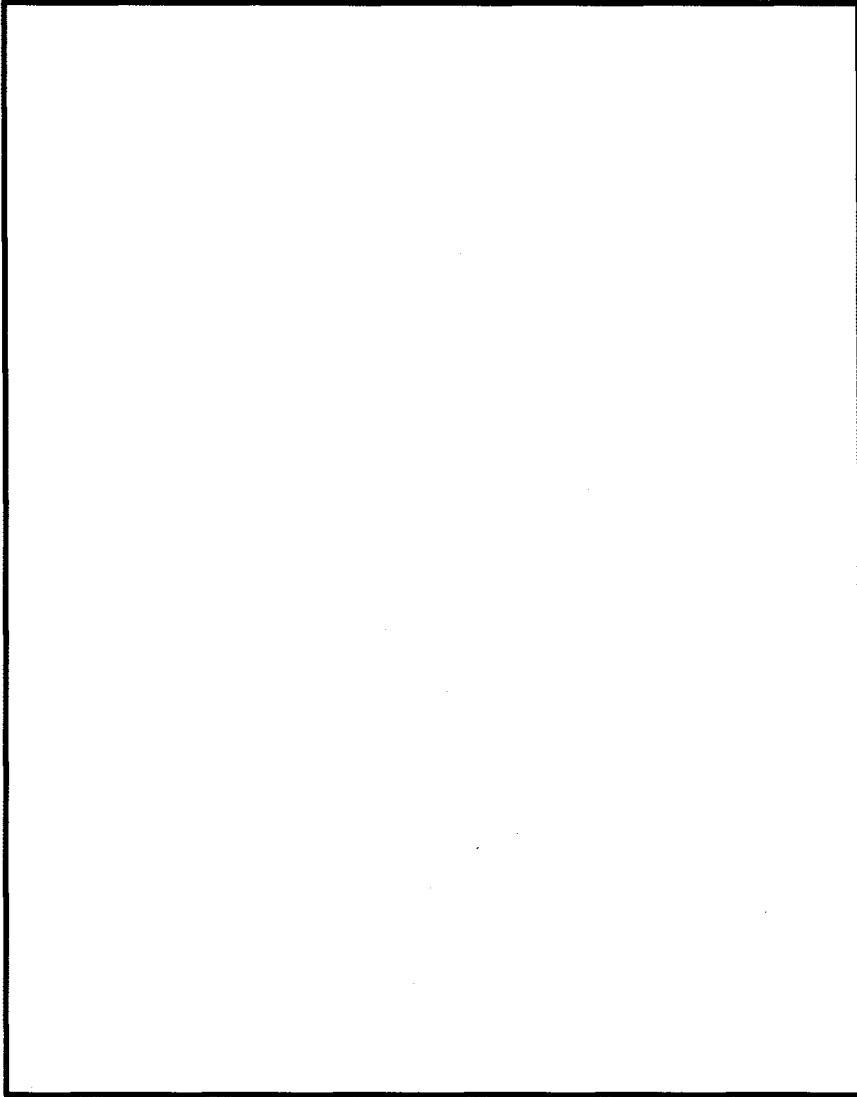
NTISSI NO. 3002

DISTRIBUTION:
NSA

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



NTISSI NO. 3002



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

~~FOR OFFICIAL USE ONLY~~
