

NTISSI No. 3008
1 May 1989

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR

TYPE I COMMUNICATIONS EQUIPMENT

CONTAINING THE FASCINATOR

SECURE VOICE MODULE (SVM)

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

1 May 1989

FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 3008, "Operational Security Doctrine for Type I Communications Equipment Containing the FASCINATOR Secure Voice Module (SVM)", establishes national standards for the use and protection of the FASCINATOR SVM.
2. This instruction is NOT RELEASABLE TO FOREIGN NATIONALS without the specific approval of the National Manager for Telecommunications and Automated Information Systems Security (NTAISS).
3. Additional copies of this instruction may be requested from:

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


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

NTISSI No. 3008

OPERATIONAL SECURITY DOCTRINE FOR COMMUNICATIONS EQUIPMENT WITH FASCINATOR

SECTION

PURPOSE AND SCOPE.....	I
REFERENCES.....	II
DEFINITIONS.....	III
EXCEPTIONS.....	IV
CLASSIFICATION GUIDANCE.....	V
ACCOUNTABILITY.....	VI
SYSTEM DESCRIPTION.....	VII
KEYING.....	VIII
PHYSICAL SECURITY.....	IX
EMERGENCY PROCEDURES.....	X
MAINTENANCE.....	XI
INCIDENTS.....	XII

SECTION I - PURPOSE AND SCOPE

1. This instruction establishes minimum national operational communications security (COMSEC) requirements for the use and protection of the Type I FASCINATOR-equipped products and associated COMSEC material. The provisions of this instruction apply to all departments and agencies of the U.S. Government and their contractors who handle, distribute, account for, store, and use these radios, products, and materials.

SECTION II - REFERENCES

2. The reference that applies to U.S. Government contractors is the U.S. Government Contractors Controlled Cryptographic Item (CCI) Manual, dated 2 February 1986.

3. The following references apply to U.S. Government departments and agencies:

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

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

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

NTISSI No. 3008

- d. NACSI No. 4008, Safeguarding COMSEC Facilities, dated 4 March 1983.
- e. NTISSI No. 4001, Controlled Cryptographic Items, dated 25 March 1985.
- f. NTISSI No. 4002, Classification Guide for COMSEC Information, dated 5 June 1986.
- g. NTISSI No. 4000, Communications Security Equipment Maintenance and Training, dated 14 July 1986.
- h. NTISSI No. 4003, Reporting COMSEC Insecurities, dated 3 November 1986.
- i. NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.

SECTION III - DEFINITIONS

4. Definitions contained in the National COMSEC Glossary (NCSC-9) apply to this instruction, with the exception that the term "COMSEC insecurity" is replaced by the term "COMSEC incident." For the purpose of this instruction the following definitions also apply:

- a. Controlled Cryptographic Item (CCI) - A secure telecommunications or information handling equipment, or associated cryptographic component, which is unclassified but controlled. Equipments and components so designated shall bear the designator controlled cryptographic item or CCI.
- b. Key - Information (usually a sequence of random binary digits) used initially to set up and to periodically change the operations performed in a crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter countermeasures (ECCM) patterns (frequency hopping or spread spectrum), or for producing other keys.

SECTION IV - EXCEPTIONS

5. Heads of departments and agencies, and their contractors, must submit requests to the Director, National Security Agency (DIRNSA) for exceptions to this doctrine where minimum standards cannot be met. All requests should be forwarded to the attention of

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

NTISSI No. 3008

SECTION V - CLASSIFICATION GUIDANCE

6. The FASCINATOR product line provides cryptographic security for voice transmissions and, when used with appropriately classified keys, is approved for the transmission of all classifications and categories of voice. When unkeyed, the FASCINATOR product line is unclassified CCI and must be protected in accordance with NTISSI No. 4001. When the equipment is keyed, it assumes the classification of the key and must be protected accordingly. It is unclassified for external viewing.

SECTION VI - ACCOUNTABILITY

7. The Secure Voice Module (SVM). The SVM is ALC-2 and requires accountability by quantity. When installed, the communications equipment which houses the SVM requires continuous accountability by serial number (ALC-1). It is recommended that the presence of such equipment be verified at least monthly. To facilitate serial number accounting of the FASCINATOR product line, a separate serial numbered stick-on label will be packaged with each module. The stick-on label will be imprinted with the following information: CCI, Motorola model number, serial number assigned by NSA, and endorsed-for-classified-traffic identifier. Placement instructions for the label will be provided on the label; once the label is affixed, it is not removable.

8. KOI-18, KYK-13, And Security Interface Box (SIB). The KOI-18, general-purpose tape reader; the KYK-13, electronic transfer device; and the SIB, the interface box between a key loader and the FASCINATOR product, are unclassified CCIs, ALC-2. When filled, the KYK-13 assumes the classification of the key.

SECTION VII - SYSTEM DESCRIPTION

9. The FASCINATOR SVMs are 12 Kbs encryption/decryption devices designed for secure voice applications. The SVMs are direct plug-in replacements for Motorola's Data Encryption Standard (DES) modules only. They are available for hand-held portables, mobile, and fixed equipment.

NTISSI No. 3008

SECTION VIII - KEYING

10. Key. The key for the FASCINATOR equipment is supplied as punched tape and is normally packaged in five segments, three copies of each, in plastic canisters. The marking, safeguarding, and control of classified key tapes and all key tapes marked CRYPTO will be in accordance with NACSI No. 4005.

11. Key Insertion. In order to load key into the FASCINATOR equipment, a SIB must be attached to the key fill connector via a cable. Key is supplied as punched tape. It may be pulled through a KOI-18 and into the SIB or it may be loaded into a KYK-13 and then into the SIB electronically.

12. Cryptoperiod. The cryptoperiod for the FASCINATOR equipment is seven days. Each COMSEC controlling authority shall establish a standard time and day of the week when the new segment for each net will be put into use. The controlling authority may authorize emergency cryptoperiod extensions of an additional week for mobile communications due to operational or logistical considerations. Cryptoperiod extensions in excess of seven days must be approved on a case-by-case basis by DIRNSA, (ATTN:). At a minimum, requests for extension should include the following information: short title of keying material, length of cryptoperiod extension, reason for extension, and net size.

13. Cryptonet Size. Cryptonets should be kept as small as operationally feasible. Generally, small cryptonets narrow the exposure of individual editions of keying material, limit the consequences of keying material compromises in terms of vulnerable communications, and lessen the problems associated with resupply. In order to maximize security and enforce need-to-know, it is advisable that key distribution be limited to users within the same community of interest.

14. Zeroization. If the FASCINATOR equipment must be left unattended and it is accessible to unauthorized users, it must be zeroized in accordance with the operating instructions (except as noted in Section IX, paragraph 17.b.(6)).

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

NTISSI No. 3008

15. Destruction of Keying Material. Keying material designated CRYPTO will be destroyed in accordance with NTISSI No. 4004. Keying material designated CRYPTO should be destroyed as soon as possible after supersession, and may not be held for longer than 12 hours following supersession. All tape segments remaining in the canister should be destroyed as soon as possible following supersession. Used tape segments should be destroyed as soon as possible after loading. The last copy of a used tape segment may be held until the end of the cryptoperiod, but must be appropriately protected and then destroyed. Since extra copies of tape segments are provided, the KYK-13 should be zeroized after successful loading.

16. The FASCINATOR equipment will be used in various situations, sometimes with only one-person control; under this circumstance, key tapes may be destroyed without a "witness of destruction" signature on the user/destruction report. This one-person destruction does not constitute a security violation or require an incident report, but should be followed only as an operational necessity and not as a user convenience. The user organization will initiate efforts to have destruction witnessed whenever possible.

SECTION IX - PHYSICAL SECURITY

17. The FASCINATOR equipment will be safeguarded in accordance with the general provisions of NTISSI No. 4001 and NACSI No. 4005, as applicable. In addition, control for keyed and unkeyed FASCINATOR equipment is as follows:

a. Unkeyed.

(1) Access to unkeyed FASCINATOR equipment, unkeyed KYK-13s, and unclassified key tapes may be granted to military and civilian employees of the U.S. Government and U.S. Government contractors whose duties require such access. Access may also be granted to military and civilian employees of foreign governments or international organizations to which the equipment has been released. In cases of jointly conducted operations involving non-U.S. Government personnel (e.g., state and local law enforcement officers), the sponsoring entity should contact DIRNSA (ATTN:), for guidance.

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

NTISSI No. 3008

(2) Outside CONUS, heads of departments or agencies or properly delegated cognizant security authorities may grant exceptions, under the conditions listed below, to permit non-U.S. citizens unescorted access to CCIs, regardless of the release status of the CCI. The approval of the National Manager must be obtained prior to allowing such access by non-U.S. citizens of countries hostile or unfriendly to the U.S. Information concerning these countries may be obtained from DIRNSA (ATTN:).

(a) Such access is in conjunction with building maintenance, custodial duties, or other operational responsibilities normally performed by such persons unescorted in the area containing the equipment.

(b) The equipment is installed within a facility which is recognized as a U.S. or combined facility, as opposed to a host nation facility, even though the primary staffing is by host nation personnel.

(c) The cognizant security authority has determined that the risk of tampering with the equipment which could result in compromise of U.S. information, is acceptable in light of the local threat and vulnerability and the sensitivity of the information being protected as indicated by its classification, special security controls, and intelligence life.

(3) Unkeyed FASCINATOR equipment will be controlled and protected in a manner that affords protection at least equal to that which is normally provided to other highly valued material (i.e., approved safes, if available, locked file cabinets, key-locked rooms, desks, containers, etc.).

b. Keyed.

(1) Access to keyed FASCINATOR equipment, keyed KYK-13 common-fill devices, and classified key tapes may be granted to military and civilian employees of the U.S. Government and U.S. Government contractors whose duties require such access and who possess appropriate U.S. Government security clearances. Contractors requiring access to U.S. classified cryptographic information must comply with appropriate directives regarding special access controls. In cases of jointly conducted operations involving non-U.S. Government personnel, (e.g., state and local law enforcement officers), contact DIRNSA (ATTN:) for guidance.

NTISSI No. 3008

(2) Access to key, keyed equipment, or fill devices may be granted to military and civilian employees of foreign governments or international organizations to which the equipment has been formally approved for foreign release if their duties require such access and they possess appropriate security clearances.

(3) In addition to all of the requirements for unkeyed CCIs (paragraph 17.a.(2)(a), (b), and (c)), the following conditions apply for unescorted access or use by foreign personnel of keyed CCIs:

(a) The foreign personnel are civilian employees of the U.S. Government or assigned to a combined facility.

(b) The foreign personnel hold a clearance issued by their government at least equal to the level of the keyed equipment.

(c) The equipment remains U.S. property and responsibility for the equipment is overseen by a U.S. citizen.

(d) The communications to be protected are determined to be essential to the support of U.S. or combined operations.

(e) U.S. users, communicating with such terminals that are operated by or in the vicinity of foreign personnel, are made aware of the non-U.S.-citizen status of the CCI user.

(f) Keying of CCIs with classified U.S. key must be done by U.S. personnel, but exceptions may be granted by DIRNSA (ATTN:). Keying of CCIs with allied key or unclassified U.S. key may be done by authorized foreign personnel.

(4) If the equipment is to be installed and operated in a foreign country at a facility which is either unmanned or manned entirely by non-U.S. citizens (in addition to the requirements of paragraphs 17.a. and b. above), special security measures may be required, e.g., vault areas, locking bars, safes, alarms, etc. Each such equipment installation must be approved in advance by DIRNSA, (ATTN:), on a case-by-case basis.

NTISSI No. 3008

NOTE: CCIs should not be moved from an environment, where the tampering risk presented by non-U.S. citizen access is acceptable, to a more sensitive environment where the risk is not acceptable. If such action is an operational necessity, the cognizant security authority must approve the move and qualified COMSEC maintenance personnel must examine all such CCIs for signs of tampering. Any evidence of tampering shall be reported as a COMSEC incident, and the CCI removed from operational use pending notification from DIRNSA.

(5) The keyed equipment must be protected in the personal custody of the user during travel away from controlled areas and appropriate storage facilities.

(6) If operational necessity should require that keyed FASCINATOR equipment, mounted in a vehicle, be left unattended, the vehicle must be locked. If unmounted (e.g., hand-held), it must be located in a locked compartment of the vehicle (e.g., trunk).

c. Transportation.

Transportation will be handled in accordance with NTISSI No. 4001.

Users should be aware of their surroundings and practice acoustical security when receiving/sending classified information to ensure that no unauthorized personnel overhear the conversation. Users should ensure that the FASCINATOR equipment is in the secure mode before transmitting classified information.

SECTION X - EMERGENCY PROCEDURES

18. An organizational contingency plan for the orderly destruction of the FASCINATOR module and key in the event of hostile overrun should be established in accordance with NTISSI No. 4004. Reasonable efforts should be made to recover the equipment and its related classified material lost through catastrophe, hostile action, or mayhem. Human life or personal injury should not, however, be risked in such recovery efforts.

NTISSI No. 3008

SECTION XI - MAINTENANCE

19. NTISSI No. 4000 contains the training requirements which apply to all persons who maintain COMSEC equipment, to include the FASCINATOR equipment. Authorized maintenance personnel need not be cleared unless they require access to classified COMSEC material/information to perform maintenance.

20. All unrepairable FASCINATOR SVMs will be destroyed in accordance with NTISSI No. 4004.

SECTION XII - INCIDENTS

21. NTISSI No. 4003 contains a general listing of reportable COMSEC incidents and reporting standards. While suspicious or unusual occurrences may or may not be compromising, they must be reported in accordance with NTISSI No. 4003 for subsequent evaluation. In addition, the following are reportable incidents:

a. Reportable Physical Incidents:

(1) Loss or unauthorized access to an SVM key tape or segment thereof, keyed SVM, or a KYK-13 containing key.

(2) Attempted or successful sabotage of, or tampering with, any of the classified SVM COMSEC materials or the fill devices.

(3) Attempted or successful unauthorized loading or extraction of SVM key.

(4) Actual or attempted maintenance of an SVM by unqualified personnel.

(5) Use of any key tape for other than its designated purpose unless approved by DIRNSA.

b. Reportable Cryptographic Incidents:

(1) User modification of the SVM, SIB, or test set without approval of DIRNSA.

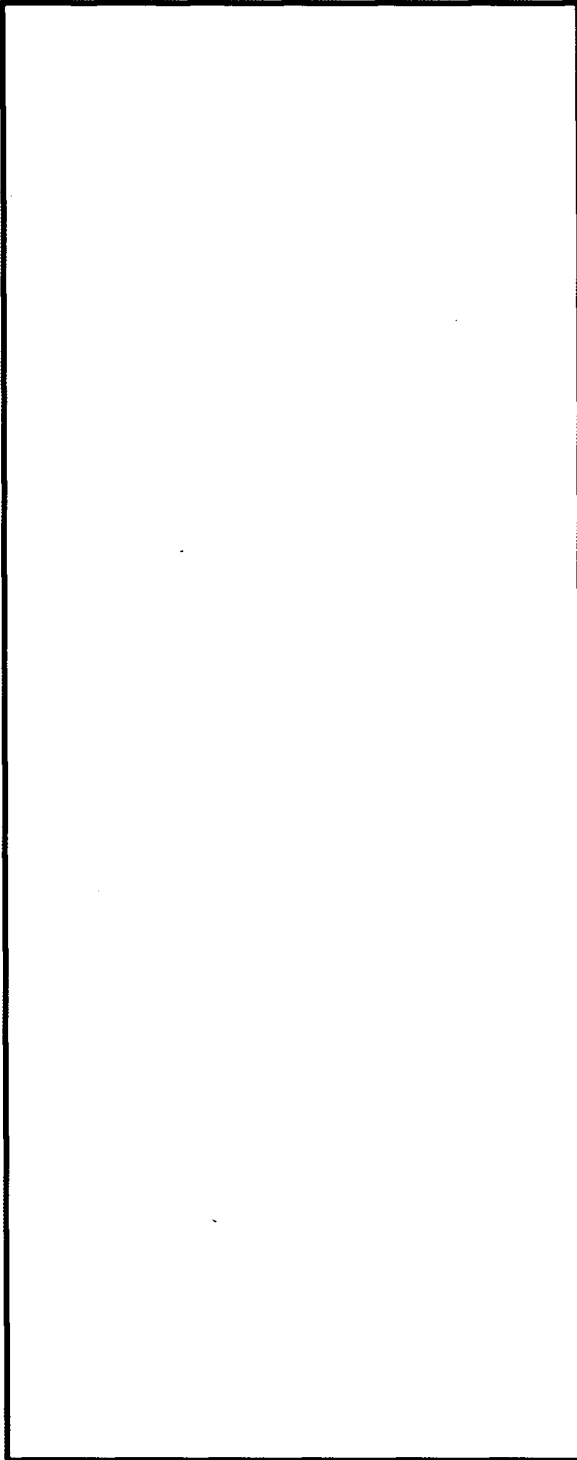
(2) Unauthorized extension of an SVM cryptoperiod.

(3) Transmission in-the-clear of information concerning the details of an SVM malfunction.

NTISSI No. 3008

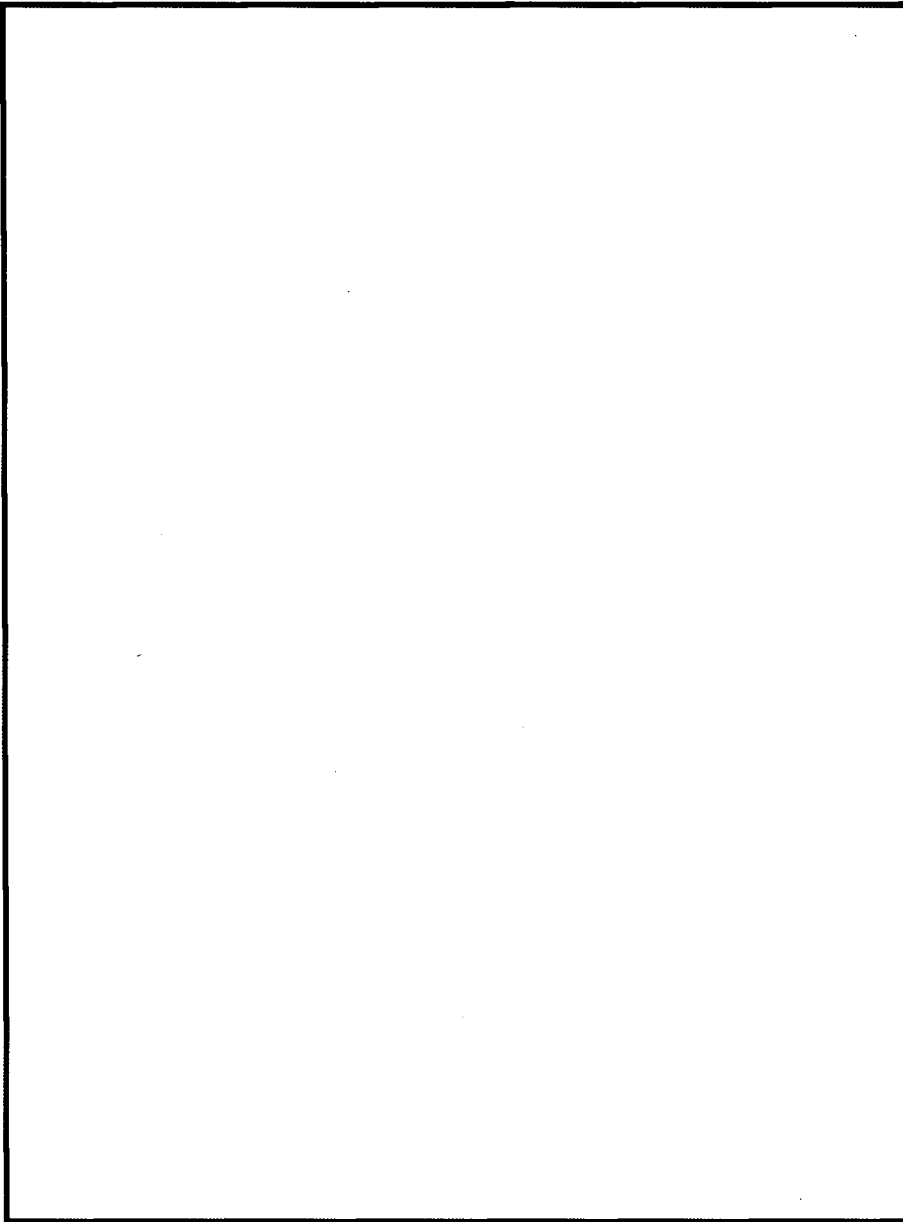
DISTRIBUTION:

NSA



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

NTISSI No. 3008



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

NTISSI No. 3008

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