~~CONFIDENTIAL~~

NTISSI No. 3001
30 October 1989

NTISS
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

OPERATIONAL SECURITY DOCTRINE

FOR THE

AUTOMANUAL SYSTEM (AMS)

~~CLASSIFIED BY DIRNSA (NATIONAL MANAGER, NTAISS)~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S~~
~~DETERMINATION REQUIRED~~

~~CONFIDENTIAL~~

NTAISS
NATIONAL
TELECOMMUNICATIONS
AND
AUTOMATED
INFORMATION
SYSTEMS
SECURITY

NATIONAL MANAGER

30 October 1989

FOREWORD

1. (U) National Telecommunications and Information Systems Security Instruction (NTISSI) No. 3001, "Operational Security Doctrine for the Automanual System (AMS)," promulgates operational security doctrine for the AMS and its associated equipment. This instruction supersedes NTISSI No. 3001, "Operational COMSEC Doctrine for the Automanual System (AMS)," dated 14 August 1986.

2. (U) This instruction and excerpts from it may be given to U.S. Government agencies or departments, the Military Services, and U.S. Government contractors. This instruction may not be given to foreign nationals without the approval of the National Manager, NTAISS.

3. (U) Heads of the Military Services and U.S. Government departments and agencies are responsible for distributing this updated NTISSI to their subordinate elements. Additional copies may be obtained from:

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

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

NTISSI No. 3001

OPERATIONAL SECURITY DOCTRINE FOR THE AUTOMANUAL SYSTEM (AMS) (U)

SECTION I - PURPOSE

1. (U) This instruction provides minimum security doctrine for the operational, secure use of AMS equipment and associated COMSEC material. Specific requirements for individual AMS equipment are contained in the annexes of this instruction. The provisions of this instruction apply to all users of AMS equipment, unless application-specific doctrine has been approved by the Director, NSA (DIRNSA).

SECTION II - REFERENCES

2. (U) Reference Listing.

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

b. NACSIM No. 5100A, Compromising Emanations Laboratory Test Requirements, Electromagnetics, dated 1 July 1981.

c. NCSC-9, National Communications Security (COMSEC) Glossary, dated 1 September 1982.

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

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

f. NTISSI No. 4003, Reporting COMSEC Insecurities, dated 3 November 1986.

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

h. NTISSI No. 4005, Control of TOP SECRET Keying Material, dated 17 July 1987.

i. NTISSI No. 4006, Controlling Authorities for COMSEC Keying Material, dated 2 May 1989.

SECTION III - DEFINITIONS

3. (U) The definitions contained in NCSC-9 apply. For the purpose of this instruction the following definition also applies: Traffic Encryption Key (TEK) - key used to encrypt plain text or to superencrypt previously encrypted text and/or decrypt cipher text.

SECTION IV - CLASSIFICATION GUIDANCE

4. (U) AMS equipment is unclassified, and is designated a controlled cryptographic item (CCI), as defined in NTISSI No. 4001, and identified by the marking CCI. NTISSI No. 4002 provides guidelines for the classification of information relative to the AMS. Descriptions of specific AMS equipment are included in the annexes to this instruction.

SECTION V - SYSTEM DESCRIPTION

5. (U) The AMS is composed of commercial grade electronic off-line cryptodevices, designed to replace selected manual cryptosystems and fulfill new off-line requirements. COMSEC doctrine and procedures for specific AMS equipment are included in the annexes to this instruction.

SECTION VI - KEYING

6. (U) AMS keying material is produced in printed, non-perforated, eight-level tape form (white). Printed on the leader of the tape is the classification, and a digraph which reflects the cryptoperiod and number of key segments in the canister. AMS keys are packaged in plastic canisters or pill boxes containing 31 separate segments.

a. Operational TEK tapes are classified on the basis of the classification of the traffic they are intended to protect. They are either regularly or irregularly superseded, depending on the system application, packaged in plastic canisters and marked CRYPTO.

b. Exercise TEK tapes, are classified on the basis of the classification of the traffic they are intended to protect. These TEK's are irregularly superseded, packaged in plastic canisters and marked CRYPTO.

c. Maintenance key tapes are either unclassified or classified and not marked CRYPTO. Maintenance key tapes are designed for back-to-back bench testing only and are not used for over-the-air transmissions. The maintenance key tapes are packaged in clear plastic pill boxes and segments may be reused until they become unusable.

d. Training key tapes are unclassified (FOR OFFICIAL USE ONLY), not marked CRYPTO, packaged in pill box containers, and may be reused until unusable. Classroom training key must not be used for over-the-air transmissions.

7. (U) Cryptoperiods relative to specific AMS equipment are included in the respective annexes of this doctrine.

8. (U) Controlling authorities for key must be aware that as the number of copies of a key grows, key management becomes more difficult and the vulnerability of that key to compromise increases. Compromise of key at one terminal potentially compromises the traffic of all users of that key during that cryptoperiod. Prescribed cryptonet sizes for specific AMS equipment are included in the respective annexes of this instruction.

9. (U) Longer cryptoperiods and larger cryptonet sizes which diverge from specific AMS doctrine must be approved on a case-by-case basis by the DIRNSA (ATTN: [redacted]

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

SECTION VII - PHYSICAL SECURITY

10. (U) AMS equipment is designated CCI and will be protected in accordance with the general provisions of NTISSI No. 4001. In addition, control requirements for unkeyed and keyed AMS equipment are as follows:

a. Because it is small and portable, an AMS device shall be afforded particular attention to ensure that access and accounting integrity are maintained.

b. Storage in a secure area for unkeyed AMS devices is encouraged; otherwise, the best protection available shall be provided. Examples of protective storage include an approved security container, a key-locked desk or cabinet within an area secured by a locked door.

c. During travel, the unkeyed AMS device will be kept in the personal possession of authorized users; otherwise, the device will be given the best protection available, e.g., temporarily locked in a car trunk. The device will be carried in the personal possession of an authorized user aboard public transportation, and not checked with baggage, unless more than one device is involved and stored baggage will be last on and first off. At airports, the attended AMS equipment may be inspected and X-rayed without compromise or damage to the logic. During transportation, the key will be physically separated from the AMS device and carried in a separate container. Both the AMS device and key may be carried by the same person. AMS devices, even when unkeyed, will not be left unattended in hotel/motel or other berthing facilities during travel.

d. Keyed AMS equipment becomes the same classification as the key and must be protected in accordance with Service or agency directives.

e. When the AMS device is used in public accommodations (hotel/motel rooms), the following applies:

(1) When used infrequently (once or twice a day) and secure storage is not available, it should be zeroized after each use and rekeyed with the same key during the same cryptoperiod.

(2) When used frequently (consistently during the cryptoperiod), it may remain keyed for the entire cryptoperiod and afforded the required physical security commensurate to the key (reference paragraph 10.d., above).

(3) The number of key segments hand receipted to travelers for use in public accommodations will vary according to the operational situation and calls for good judgment on the part of the controlling authority. Issuing a full key canister for a short trip may subject key for large nets to

possible compromise if lost or stolen. If travelers expect to use fewer than seven key segments for such large nets, it is better to remove the required key segments from the canister for issue.

11. (U) AMS keying material must be controlled in accordance with the provisions of NACSI No. 4005 and NTISSI No. 4005. In addition:

a. During travel away from controlled areas and where appropriate storage facilities are unavailable, the key must be protected in the personal custody of the user.

b. AMS device key storage positions will be used to participate in multiple nets, where required, and will not be used to store future key unless such application is approved for special mission purposes by the responsible controlling authority.

c. It is understood that AMS devices will 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 insecurity report. This scenario may be followed as an operational necessity and not as a user convenience.

SECTION VIII - EMERGENCY PROCEDURES

12. (U) Refer to NTISSI No. 4004, "Routine Destruction and Emergency Protection of COMSEC Material," dated 11 March 1987, for destruction and emergency protection requirements.

SECTION IX - REPORTABLE INCIDENTS

13. (U) Reportable incidents are addressed in NTISSI No. 4003, "Reporting COMSEC Insecurities," dated 3 November 1986.

2 Encls:
1. Annex A, TSEC/KL-42 Automanual Equipment
2. Annex B, TSEC/KL-43 Automanual Equipment

ANNEX A

TSEC/KL-42 AUTOMANUAL EQUIPMENT

SECTION I - SYSTEM DESCRIPTION

1. (U) The TSEC/KL-42 is a portable, electronic, off-line crypto-equipment for encryption/decryption of alphanumeric information of all categories and classifications, and a user option authentication capability for challenges and replies. It has a built-in keyboard for information input, a liquid crystal display (LCD), a built-in modem and a telephone handset coupler for transmission/receipt of encrypted/decrypted data over standard telephone lines, and printer connection capability. The KL-42 is not a ruggedized device.

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

SECTION II - PROCEDURES

2. (U) The KL-42 without a printer, or with an approved printer, is authorized for unrestricted use for classifications up to and including TOP SECRET, within the constraints of Section IV below. Approved printers compatible with the KL-42 are included in the Information Systems Security Products and Services Catalogue. Other compatible printers and restrictions on their use are included in a separate list available from the DIRNSA (ATTN: [redacted]). Printers not on these lists will not be used unless exploitation is deemed highly improbable by the responsible security authority.

3. (U) Since KL-42 printers do not automatically mark printed messages with the classification level, a statement of classification shall be included in printed messages processed by the KL-42.

4. (U) If knowledge of the time a message is sent is critical to proper interpretation of the message, that message shall include a date/time/message count feature in the plain text.

5. (U) KL-42 encrypted messages may be transmitted via any medium (Morse code, verbal, modem, etc.).

SECTION III - KEYING

6. (U) KL-42 traffic encryption keys (TEK) are operational key or exercise key having a 24-hour

cryptoperiod. Each 31-segment TEK canister is superseded monthly. A used TEK tape segment may be retained up to 72 hours after its cryptoperiod to accommodate delayed messages (NTISSI No. 4004 applies); however, the key must be protected to preclude traffic compromise through loss or espionage until its destruction. KL-42 classroom training key and maintenance key have no cryptoperiod and each key segment may be reused until unusable. Classroom training key and maintenance key will not be used for over-the-air transmissions.

7. (U) Cryptonets for the KL-42 are by necessity large. In such cases, KL-42 cryptonets are limited to 200 members when traffic is TOP SECRET and up to 1000 members when traffic is SECRET and lower. Larger nets must be approved on a case-by-case basis by the DIRNSA (ATTN: [redacted]).

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

SECTION IV

SECURITY REQUIREMENTS FOR USE OF THE KL-42 DEVICES

8. ~~(C)~~ [redacted]

9. ~~(C)~~ [redacted]

a. [redacted]

b. [redacted]

c. [redacted]

10. ~~(C)~~ [redacted]

ANNEX A to
NTISSI No. 3001

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

11. ~~(C)~~ [redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

12. ~~(C)~~ [redacted]

ANNEX B

TSEC/KL-43 AUTOMANUAL EQUIPMENT

SECTION I - SYSTEM DESCRIPTION

1. (U) The TSEC/KL-43 is a portable, electronic, off-line crypto-equipment for encryption/decryption of alphanumeric information of all categories and classifications, and a user option authentication capability for challenges and replies. It has a built-in keyboard for information input, a liquid crystal display (LCD), a built-in modem and a telephone handset coupler for transmission/receipt of encrypted/decrypted data over standard telephone lines, and printer connection capability. The KL-43 has a built-in special application keyboard for daily key updating. In this annex, KL-43 equipment indicates any crypto-equipment in the KL-43 family, including the KL-43, KL-43A, KL-43C ruggedized device, and KL-43D. The KL-43 system is not interoperable with the KL-42 system; however, the key used for the KL-43 is the same format as the key used with the KL-42. The KL-43 and KL-43A models are not interoperable with other KL-43 models (e.g., KL-43C and KL-43D) when the update feature is used. They are interoperable in all other modes. Holders of the KL-43 family no longer need prior NSA approval for use of the update feature.

SECTION II - PROCEDURES

2. (U) The KL-43 without a printer, or with an approved printer, is approved for use for classifications up to and including TOP SECRET, within the constraints of Section IV below. Approved printers compatible with the KL-43 are included in the Information Systems Security Products and Services Catalogue. Other compatible printers and restrictions on their use are included in a separate list available from the DIRNSA (ATTN: [redacted]).

3. (U) Since KL-43 printers do not automatically mark printed messages with the classification level, a statement of classification shall be included in printed messages processed by the KL-43. (Note: In the plaintext word processor mode, the KL-43 always prompts the entry of a message classification.)

4. (U) If knowledge of the time a message is sent is critical to proper interpretation of the message, that message

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

shall include a date/time/message count feature in the plain text.

5. (U) KL-43 encrypted messages may be transmitted via any medium (Morse code, verbal, modem, etc.).

SECTION III - KEYING

6. (U) KL-43 traffic encryption keys (TEK) are operational key or exercise key having either a 24-hour cryptoperiod or weekly cryptoperiod when using the daily key update feature. Each 31-segment TEK canister is superseded monthly when using the 24-hour cryptoperiod or superseded every 6 months when using the daily key update feature with the weekly cryptoperiod. A used TEK tape segment may be retained up to 72 hours after its cryptoperiod to accommodate delayed messages (NTISSI No. 4004 applies); however, the key must be protected to preclude traffic compromise through loss or espionage until its destruction. KL-43 training key and maintenance key have no cryptoperiod and each key segment may be reused until unusable. Training key and maintenance key will not be used for over-the-air transmissicns. All KL-43 and KL-42 key tapes are compatible even though the equipment is not.

7. (U) Cryptonets for the KL-43 are by necessity large. KL-43 cryptonets employing a 24-hour cryptoperiod shall be kept to 200 users for TOP SECRET and 1000 users for SECRET and lower. If the daily key update feature is used, the cryptoperiod is weekly (7 days), and cryptonets shall be kept to 30 users for TOP SECRET and 150 users for SECRET and lower. Larger nets and/or longer cryptoperiods must be approved by the DIRNSA (ATTN: [redacted]).

8. (U) All KL-43 equipment has a capability of updating 35 times before a new key (TEK) must be applied. Under some mission scenarios, updating is required after each message is processed. This procedure will provide added security for message protection but is determined by the users' controlling authority. Also, the controlling authorities have the following options:

a. Keying every 24 hours with no updates;

b. Updating after every message for 35 updates within the 24-hour cryptoperiod;

c. A 7-day cryptoperiod with daily updates.

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

9. (U) If an equipment malfunction in the encryption or decryption process occurs, change the KL-43 equipment, rekey that equipment with the TEK tape for that cryptoperiod, and update to the appropriate day (if updating). Malfunction is defined as a function that will not clear in the encryptor, or failure of the decryptor to achieve cryptosynchronization.

SECTION IV

SECURITY REQUIREMENTS FOR USE OF THE KL-43/KL-43A AND KL-43D

10. ~~(C)~~ [redacted]

11. ~~(C)~~

12. ~~(C)~~

a.

b.

c.

13. ~~(C)~~

14. ~~(C)~~

ANNEX B to
NTISSI No. 3001

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

a. [redacted]

b. [redacted]

c. [redacted]

[redacted]

d. [redacted]

[redacted]

15. ~~(C)~~ [redacted]

[redacted]

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

DISTRIBUTION:
NSA

[redacted]

[redacted]

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