5 August 2003

Secretariat Manager

CNSS-079-03

MEMORANDUM FOR DISTRIBUTION

SUBJECT: (U//~~FOUO~~) Amendment to NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, dated August 1997

(U) Please make the following pen-and-ink changes to NSTISSI No. 4005.

a. (U//~~FOUO~~) Change that portion of paragraph 16 (Facility Security) that reads: "...must be secured with an approved electro-mechanical lock meeting Federal Specification FF-L-2740."

To read: "...must be secured with a three position, changeable combination padlock meeting Federal Specification FF-P-110."

b. (U//~~FOUO~~) Change that portion of paragraph 29.a (Unattended Telecommunications Facilities) that reads (original version): "...or equipped with lockbars secured by a (*sic*) electro-mechanical lock meeting Federal Specification FF-L-2740."

To read: "...or equipped with lock bars secured by three position, changeable combination padlocks meeting Federal Specification FF-P-110."

c. (U//~~FOUO~~) Change paragraph 43.c to read: "Aboard ships, in a steel filing cabinet having a lock bar secured by a three position, changeable combination padlock meeting Federal Specification FF-P-110."

CNSS Secretariat [redacted] - National Security Agency ~ 9800 Savage Road STE 6716 ~ Ft Meade MD 20755-6716

[redacted]

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

d. (U//~~FOUO~~) Change that portion of paragraph 76.b that reads: "...the keyed equipment may be protected by lockbars secured by an electro-mechanical lock meeting Federal Specification FF-L-2740..."

To read: "...the keyed equipment may be protected by lock bars secured by three position, changeable combination padlocks meeting Federal Specification FF-P-110..."

(U) This amendment is necessary since the FF-P-110 is a specification for combination padlocks that are used to secure locking bars and hasps. FF-L-2740 is a specification for built-in changeable combination locks that are used to secure vault doors and the like. The use of FF-L-2740 throughout NSTISSI No. 4005 was not appropriate in several instances.

(U) This amendment is effective immediately.

[redacted] (b)(3)-P.L. 86-36

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

NSTISSC-003-98

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Amendment to NSTISSI 4005 Safeguarding COMSEC Facilities and Material - **ACTION MEMORANDUM**

Please make the following change to NSTISSI 4005, dated Aug 97. This amendment specifically outlines the special handling instructions regarding the transportation of TOP SECRET key:

Add to paragraph 85., a.: Whenever local couriers transport TOP SECRET keying material from a user COMSEC account to another user account or user location, two-person integrity controls shall be applied. Receipts for this material must be signed by two persons who are cleared for TOP SECRET and are authorized to receive the material. While in the custody of the Armed Services/ Defense Courier Service or the Diplomatic Courier Service, two-person integrity controls are not required for TOP SECRET keying material.

KENNETH A. MINIHAM
Lieutenant General, USAF

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

NSTISSI No. 4005
August 1997

SAFEGUARDING COMMUNICATIONS SECURITY (COMSEC) FACILITIES AND MATERIALS

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

NATIONAL MANAGER

FOREWORD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, establishes the minimum national standards for constructing and protecting COMSEC facilities wherein the primary purpose is generating, storing, repairing, or using COMSEC material. These standards apply only to the aforementioned types of facilities. NSTISSI No. 4005 also establishes the minimum national standards for safeguarding COMSEC material; these standards apply to all COMSEC material controlled within the COMSEC material control system (CMCS) regardless of the purpose of the facility in which it is used. (In addition to prescribing the minimum national requirements (identifiable by the words "will" or "must"), this NSTISSI presents guidelines (identifiable by the words "shall", "should", "may" or "can") for protecting COMSEC material.)

2. This instruction consolidates and supersedes NTISSI No. 4005, Control of Top Secret Keying Material, dated 17 July 1987; NACSI No. 4008, Safeguarding COMSEC Facilities, dated 4 March 1983; and NACSI No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.

3. 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.

4. Comments and suggestions regarding this NSTISSI may be directed to the NSA [redacted]

KENNETH A. MINIHAN
Lieutenant General, USAF

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

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

[redacted]

SAFEGUARDING COMSEC FACILITIES AND MATERIALS

SECTION

PURPOSE I
SCOPE II
POLICY III
EXCEPTIONS IV
RESPONSIBILITIES V
MOBILE COMSEC FACILITIES VI
FIXED COMSEC FACILITIES VII
PHYSICAL SECURITY OF COMSEC MATERIAL VIII
STORAGE OF COMSEC MATERIAL IX
COMSEC MANAGERS/COMSEC CUSTODIANS X
ACCOUNTING, INVENTORY, AND AUDITS XI
THE PROTECTIVE TECHNOLOGIES INSPECTION PROGRAM XII
ISSUING AND USING COMSEC MATERIAL XIII
TRANSPORTATION OF COMSEC MATERIAL XIV
PROTECTING PASSWORDS AND LOCK COMBINATIONS XV
ALTERATION AND REPRODUCTION XVI

SECTION I - PURPOSE

1. This National Security Telecommunications and Information Systems Security Instruction (NSTISSI) prescribes the minimum national requirements for the construction, approval, and security of facilities wherein the primary purpose is generating, storing, repairing, or using communications security (COMSEC) material. This NSTISSI also establishes the minimum national requirements for safeguarding and controlling COMSEC material; these requirements apply to all COMSEC material controlled within the COMSEC material control system (CMCS), regardless of the purpose of the facility in which it is used. Heads of appropriate departments and agencies, or their designees, may impose additional requirements on elements under their cognizance.

SECTION II - SCOPE

2. The requirements of this NSTISSI apply to all U.S. Government Executive Branch departments, agencies, and their contractors, consultants, and licensees who own, procure, use, operate, or maintain national security systems as defined by NSTISSD No. 502 (reference a.). Its specific requirements apply to all COMSEC material used to secure national security systems, irrespective of form or generation process.

SECTION III - POLICY

3. Implementation can be accomplished by issuing this NSTISSI in its entirety or by incorporating its provisions into department or agency directives. Where joint or unified commands or programs encounter conflicting COMSEC implementing directives, this NSTISSI will take precedence.

4. When the requirements or terms of this instruction appear to substantially conflict with the requirements or terms of any other national-level issuance, this conflict will be identified and guidance requested, through organizational channels, from the National

Manager, National Security Telecommunications and Information Systems Security (NSTISS) (Director, National Security Agency, ATTN: INFOSEC Policy and Doctrine Division).

5. COMSEC information not specifically covered by this NSTISSI must be safeguarded and controlled in accordance with department or agency directives for safeguarding and handling other U.S. Government information of the same classification.

6. To the extent specified in this NSTISSI the publications listed in ANNEX A apply.

7. The definitions in ANNEX B have been extracted from NSTISSI NO. 4009 (reference b.) and information pertaining only to this NSTISSI are added in brackets after each definition.

SECTION IV - EXCEPTIONS

8. NATO Nuclear Command and Control COMSEC Material is safeguarded and controlled as described in AMSG-773 (reference c.). Other NATO material is safeguarded and controlled as prescribed in AMSG-293 (reference d.) and AMSG-505 (reference e.).

9. Joint Staff positive control material and devices (i.e., Sealed Authenticator System, Permissive Action Link, Coded Switch System, Positive Enable System, and Nuclear Certified Computer Data) are safeguarded and controlled as prescribed in Chairman Joint Chiefs of Staff Instruction, CJCSI 3260.01 (reference f.).

10. Unkeyed equipment designated controlled cryptographic items (CCI) is safeguarded and controlled as prescribed in NSTISSI No. 4001 (reference g.).

11. COMSEC facilities holding only manual cryptosystems for tactical applications, unclassified keying material for machine cryptosystems, or publications other than full maintenance manuals are exempt from the construction requirements of this NSTISSI.

12. National standards delineated in this instruction do not alter or supersede existing authorities of the Director of Central Intelligence (see NSTISSD No. 502, reference a.).

SECTION V - RESPONSIBILITIES

13. Heads of appropriate departments and agencies shall:

a. Ensure the requirements of this NSTISSI are met, either through strict compliance or the use of alternative arrangements. (Alternative arrangements must satisfy the intention of the original requirement. An information copy of all alternative arrangements must be sent to the National Manager, National Security Agency, ATTN: [redacted]

b. Establish a CMCS including, but not limited to, a Central Office of Record (COR) and supported COMSEC accounts;

c. Establish procedures ensuring COMSEC managers/custodians and assistant COMSEC managers/custodians are properly appointed and trained, and their clearances are verified; and

d. Establish a protective technologies inspection program meeting the requirements set forth in SECTION XII of this NSTISSI.

[redacted]

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

14. The National Manager shall:

a. Interpret the standards of this NSTISSI and provide guidance about alternative arrangements;

b. Have authority to waive requirements contained in this NSTISSI and approve alternative arrangements, when strict adherence to a requirement would impede mission effectiveness;

c. Ensure the development, evaluation, and production of protective technologies for information processing equipment and keying material;

d. Establish a national protective technologies inspection and detection center providing comprehensive protective technologies products, information, training, technical guidance, and inspection services and assistance; and

e. Ensure the development and distribution of instructional guidance and procedures for the installation, maintenance, inspection, and secure disposal of protective technologies applied to information processing equipment and keying material (usually published as protective technologies pamphlets).

SECTION VI - MOBILE COMSEC FACILITIES

15. This section contains requirements and special allowances unique to mobile COMSEC facilities. If a mobile COMSEC facility is operational in a fixed location for three months or longer, it is considered a fixed COMSEC facility, and all requirements for fixed COMSEC facilities except construction apply. Mobile COMSEC facilities temporarily moved (for five working days or less) to perform maintenance, maintain vehicle operability, etc., and then returned to the previous location will be treated as fixed facilities.

16. Facility Security - Where a mobile COMSEC facility is contained within a solid enclosure (e.g., van or shelter), all access points other than the entrance door must be secured from inside the facility, and the entrance door must be secured with an approved electro-mechanical lock meeting Federal Specification FF-L-2740. Where this is not feasible, approved locking bars or other locking devices should be used on equipment racks to deter and detect removal of, or tampering with, the COMSEC equipment. Unattended mobile facilities containing unencrypted keys, codes, or authenticators must be guarded in accordance with the requirements of paragraph 32, below.

17. Mobile Facilities - Should be in areas having a single access control point. Access control points must be protected in a manner commensurate with the threat as determined by the local commander or responsible official.

18. Requirements for Aircraft Containing COMSEC Material - Due to space limitations, it will not always be possible for U.S. guards to accompany a flight. When air crews layover in non-allied countries, and U.S. guards are not available, air crews must attempt to have classified keying material transported to a U.S. facility for secure storage. If this is not possible, COMSEC material may remain onboard the aircraft, but the following requirements must be strictly adhered to. Guards employed by the host country may be used for area control only.

a. COMSEC equipment must be zeroized or contain only encrypted key. If the equipment is filled with encrypted key, the crypto-ignition key (CIK) must be removed or configured, so it cannot be operated by unauthorized personnel.

b. All superseded keying material not protectively packaged, and keying material being removed from its protective packaging, must be destroyed or removed for personal custody by a crew member.

c. All remaining keying material must be secured in a department or agency-approved container mounted in or internally chained to the aircraft structure.

d. Aircraft and container must be locked. If the aircraft is not lockable, the doors must be sealed. Use of evidence tape is an acceptable method for sealing an aircraft. The aircraft and container must be checked by U.S. personnel at least daily for aircraft parked on either military or civilian airfields within the United States, its territories and possessions. Aircraft parked on other airfields must be checked at least every 12 hours for signs of tampering or penetration. Any suspected tampering must be reported in accordance with the requirements of NSTISSI No. 4003 (reference h.). The abbreviated reporting procedures for tactical deployments may be followed.

SECTION VII- FIXED COMSEC FACILITIES

19. This section contains requirements and special controls unique for fixed COMSEC facilities. Work areas not considered COMSEC facilities, which contain COMSEC equipment (e.g., STU-III, KG-84, Data Transfer Device [DTD]), must be protected in a manner affording protection at least equal to what is normally provided to other high value/sensitive material, and ensuring access and accounting integrity is maintained.

20. Location - Fixed COMSEC facilities should be located in areas permitting access control and as far away as possible from areas difficult or impossible to control.

21. Construction - All fixed COMSEC facilities must be constructed of material that will deter and detect covert penetration. Facilities must be constructed so that classified information cannot be overheard through walls, doors, windows, ceilings, air vents, and ducts, when secure areas border on unsecure areas. The remaining requirements of this section are not applicable to continuously attended bulk encryption facilities. However, continuously attended bulk encryption facilities must adhere to all requirements for storage of COMSEC material and protection of unattended COMSEC equipment. Heads of appropriate departments and agencies, or their designees, may approve alternative construction standards when supplemental security systems (e.g., intrusion alarms, armed guards, video cameras, etc.) are used.

a. Walls, Floors, and Ceilings - Outer walls, floors, and the ceiling of the building will be permanently constructed and attached to each other. All construction must be done in such a manner as to provide visual evidence of unauthorized penetration. All openings shall provide sufficient sound attenuation precluding inadvertent disclosure of conversation. Director of Central Intelligence Directive (DCID) 1/21, Annex A, (reference i.) will be referred to as the national standard for acoustical control and sound masking techniques.

b. Main Entrance Door - Only one door should be used for regular entrance to the facility. The door must be strong enough to resist forceful entry. In order of preference, examples of acceptable doors are GSA-approved vault doors; standard 1 3/4 inch, internally reinforced, hollow metal industrial doors; and metal-clad or at least 1 3/4 inch thick solid hardwood doors. The door frame must be securely attached to the facility and fitted with a heavy-duty/high-security strike plate, and hinges installed with screws long enough to resist removal by prying. The door must be installed to resist the removal of the hinge pins by locating the hinge pins inside the facility or by set screwing or welding the pins in place.

c. Other Doors - May exist for emergency exit and for moving bulky items. These doors must meet the construction criteria of the main entrance door and must be designed so they can be opened only from inside the facility. Approved panic hardware, intrusion detection, and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility. Emergency escape mechanisms that by pass the built-in combination lock should be double-latched. All doors must remain closed during facility operations and must be opened only for passage of authorized personnel or material.

d. Door Lock - The main entrance door to facilities not continuously attended must be equipped with a GSA-approved electro-mechanical lock meeting Federal Specification FF-L-2740. A built-in lock is not required for facilities continuously attended; however, the door must be able to accommodate a combination electro-mechanical lock meeting Federal Specification FF-L-2740 and dead bolt should it ever become necessary to lock the facility from the outside. An electronically actuated lock (e.g., cipher lock or keyless push button lock) may be used on the entrance door to facilitate the admittance of authorized personnel when the facility is attended. However, these locks do not afford the required degree of protection and may not be used to secure the facility, when it is not attended. Facility occupants must maintain positive control of the entrance at all times, regardless of the locking mechanism.

e. Windows - COMSEC facilities should not contain windows. Where windows exist affording visual surveillance of personnel, documents, materials, or activities within the facility, the window shall be made opaque or equipped with blinds, drapes, or other coverings precluding such visual surveillance. Windows less than 18 feet above the ground, measured from the bottom of the window, or are easily accessible by means of objects directly beneath the window, will be constructed from or covered with materials that will provide protection from forced entry. Facilities located within fenced and guarded government compounds or equivalent may eliminate this requirement, if the windows are made inoperable by either permanently sealing them or equipping them on the inside with a locking mechanism.

f. Other Openings - Air vents, ducts, or any similar openings, breaching the walls, floor, or ceiling of the facility, must be appropriately secured to prevent penetration. Openings less than 96 square inches must have approved baffles installed to prevent an audio or acoustical hazard. If the opening exceeds 96 square inches, acoustical baffles must be supplemented by either hardened steel bars or an approved intrusion detection system.

22. COMSEC Vaults - Are used as storage facilities for COMSEC keying material must be constructed in accordance with the standards of reference i.

23. COMSEC Facility Inspections - The inspections required in the remaining paragraphs of this section should be conducted by individuals not directly involved in the installation, operations, or maintenance of the facility. COMSEC managers/custodians cannot inspect their own facility and, whenever possible, inspectors should be of an organization other than the one being inspected. All required inspections must be documented and records kept on file at the facility and the cognizant security office, for at least three years.

24. COMSEC Facility Approval

a. Initial Inspection - Every fixed COMSEC facility must be approved by the responsible department or agency before the facility may hold classified COMSEC material. Approval must be based on a security inspection determining the facility meets the requirements for safeguarding COMSEC material, as prescribed in this NSTISSI.

b. COMSEC Facility Reinspections - After initial approval, periodic reinspections will be conducted based on threat, physical modifications, sensitivity of programs, and past security performance. Unattended telecommunications facilities should be inspected [redacted] intervals, confirming the integrity of the facility; these inspections must be performed by competent U.S. personnel only. The facility must also be reinspected and approval confirmed when there are indications of penetration or tampering, after alterations significantly changing the physical characteristics of the facility, when the facility is relocated, or when the facility is reoccupied after being temporarily abandoned. Any suspected tampering must be reported in accordance with the requirements of reference h.

25. COMSEC Inspections - A COMSEC inspection should be conducted prior to initial activation where practical, but must be conducted within 90 days after activation. Thereafter, facilities must be reinspected based on threat, physical modifications, sensitivity of programs, and past security performance. At a minimum, the inspection must address secure operating procedures and practices, handling and storage of COMSEC material, and routine and emergency destruction capabilities.

26. Technical Security Evaluation (TSE) - All reasonable countermeasures should be taken to ensure there are no clandestine surveillance devices in COMSEC facilities. Evaluations for clandestine surveillance devices should be conducted as appropriate to the threat level determined by the cognizant security office. Such evaluations should be considered when facilities are initially activated or reactivated after foreign occupation, there is known or suspected access by foreign maintenance or construction personnel, or clandestine surveillance or recording devices are suspected in or near a COMSEC facility. Any actual or suspected clandestine surveillance or recording devices must be reported in accordance with the requirements of reference h.

27. TEMPEST Countermeasures and Verifications - TEMPEST countermeasures will be determined in accordance with the requirements of reference j. Appropriate verification procedures will be conducted periodically, as determined by department or agency policy, based on the amount and sensitivity of the information processed.

28. Intrusion Detection Systems - Each intrusion detection system installed for the protection of COMSEC material must meet GSA-approved alarm system component specifications, where available, and be approved and certified by the using department or agency. The system must be capable of detecting access at each entry point or area requiring protection. The system should have an emergency backup power system, which may consist of either battery and/or generator power complying with underwriter laboratory (UL-603) specifications, and must alarm in an attended area where a guard can be dispatched within five minutes.

29. Special Security Controls

a. Unattended Telecommunications Facilities - Unattended telecommunications facilities must be protected by an intrusion detection system or guarded in accordance with the requirements of paragraph 32 of this NSTISSI. Where an intrusion detection system is employed and more than15 minutes are required to respond to an alarm, the COMSEC equipment in use should have remote zeroization capability. Personnel who visit unattended facilities should inspect the facilities for signs of tampering or attempted penetration. Signs of attempted or actual penetration must be reported in accordance with the requirements of reference h. Keyed COMSEC equipment must be secured in a container approved by NSA for closed-door operation or equipped with lockbars secured by a electro-mechanical lock meeting Federal Specification FF-L-2740. Maintenance manuals will not be

stored in unattended facilities. Only operationally required equipment may be held at unattended facilities. Only key installed in the equipment may be kept at unattended facilities.

b. Bulk Encryption Facilities - Bulk encryption facilities not continuously attended must be equipped with intrusion detection systems.

30. Visitor Register - A visitor register must be maintained at the facility entrance area recording the arrival and departure of authorized visitors. This register should contain the information listed below and must be retained for at least one year:

a. Date and time of arrival and departure:

b. Printed name and signature of visitor:

c. Purpose of visit: and

d. Signature of authorized individual admitting visitor.

SECTION VIII - PHYSICAL SECURITY OF COMSEC MATERIAL

31. Daily Security Check - In facilities other than unattended telecommunications facilities, a security check should be made at least once every 24 hours. The security checks should be conducted on a random basis to prevent a pattern from developing in the event the facility is under surveillance.

a. In a continuously attended facility, there should be a visual check once per shift ensuring all COMSEC material is properly safeguarded and physical security systems or devices (e.g., door locks and vent covers) are functioning properly.

b. In a facility not continuously attended, the security check should be conducted prior to departure of the last person. The check should ensure all COMSEC material is properly stored, that cabinets and security containers are properly secured, and the area is secured against unauthorized access. The last person to depart should ensure the facility entrance door is locked and intrusion detection systems are activated where installed.

c. If a facility is in an area posing a high risk of capture by an adversary and will be unattended for periods greater than 24 hours, it should be protected by an intrusion detection system. A check must be made at least once every 24 hours ensuring all doors to the facility are locked and there have been no attempts at forceful entry.

32. Guards

a. When guards are used to provide physical security, they must be responsible and trustworthy personnel, who have been instructed concerning their

responsibilities. Guards may be armed in accordance with department or agency procedures and local laws or status of forces agreements.

b. Guards whose duties include access to COMSEC material must meet the access requirements of this NSTISSI. Guards who are not given access to COMSEC material and are used to supplement other physical security measures (e.g., approved security containers or locks) need not meet access requirements. If a facility is located in U.S. or allied territory, a roving guard making rounds at least every four hours is sufficient as long as the COMSEC material is appropriately secured. In allied countries, guards employed by the host

country may be used for area control. If a facility is located in non-U.S., non-allied territory, U.S. guards must be used and must be situated at all times in the immediate area of the facility, preferably within the facility.

33. Nonessential Audio/Visual Equipment

a. Personally Owned Equipment

(1) The following personally owned electronic equipment may be introduced into a COMSEC facility:

(a) Calculators, spell-checkers, wrist watches, and data diaries;

NOTE: If equipped with data-ports, the cognizant security officer will ensure that procedures are established to prevent unauthorized connection to automated information systems.

(b) Receive-only pagers and beepers;

(c) Audio and video equipment with only a "playback" feature (no recording capability) or with the "record" feature disabled/removed; and

(d) Radios.

(2) The following electronic equipment items are prohibited in COMSEC facilities:

(a) Personally owned photographic, video, or audio recording equipment; and

(b) Personally owned computers and associated media.

b. Government-owned or leased Equipment

The following U.S. Government owned or leased (or company owned or leased) items are prohibited in COMSEC facilities unless approved by the cognizant security officer for conduct of official duties:

(1) Two-way transmitters;

(2) Audio, video, or optical recorders; and

(3) Test, measurement, and diagnostic equipment.

34. Access to COMSEC Material

a. U.S. citizens may be granted access to TOP SECRET or SECRET COMSEC material if they are employees of the U.S. Government having an appropriate security clearance and the need-to-know. U.S. citizens having access to TOP SECRET and SECRET cryptographic material must be briefed and sign a cryptographic access certificate in accordance with the requirements of NTISSP No. 3 (reference k.). U.S. citizens may be granted access to CONFIDENTIAL COMSEC material, if they have the appropriate clearance and their duties

require access. Clearances are not required for access to unclassified cryptographic material or encrypted traffic encryption key (TEK); however, access must be restricted to persons with a need-to-know. Individuals must be properly indoctrinated in accordance with the following: national policy and department and agency rules and regulations regarding the sensitivity of the material; the rules for safeguarding such material; the laws pertaining to espionage; the procedures for reporting COMSEC incidents; and the rules pertaining to foreign contacts, visits, and travel.

b. Contractors and nongovernment persons acting at the direction of the U.S. Government may be granted access within the provisions of NCSC-2 (reference l. and reference k.).

c. Resident aliens who are U.S. Government civilian or military personnel may have access to unclassified COMSEC material, if their duties require it. Resident aliens may have access to CONFIDENTIAL COMSEC material, if they have a clearance based on a successful background investigation and indoctrination and their duties require such access. They may not be appointed COMSEC manager/custodian or have access to areas where COMSEC material is stored.

d. Foreign nationals representing a foreign government or international organization may be given access to COMSEC information specifically released to the represented government or organization under the provision of NSTISSP No. 8 (reference m.). Before any release is made, the foreign government or organization must state in writing that the representative has an appropriate clearance and is officially designated to receive the information.

e. When an unclassified cryptosystem is unavailable or inappropriate, uncleared U.S. Government employees or contractors may use classified cryptosystems under the supervision of an appropriately cleared person, if the uncleared user requires use of the system in the performance of his or her duties. The distant-end must be notified that an uncleared person is using the equipment, and sufficient safeguards exist to prevent access to the classified components of the cryptosystems.

f. Uncleared repair personnel admitted to perform maintenance on commercially contracted information-processing equipment connected to circuits protected by COMSEC equipment must be escorted. The escort should be a COMSEC maintenance person or other qualified individual capable of determining if a malicious action has been taken against the involved COMSEC equipment or the installation configuration. Other uncleared personnel (construction, cleaning, etc.) required to access the facility must be escorted at all times.

35. Access to Keying Material Designated for Encryption of Sensitive Compartmented Information (SCI) - Access to keying material used to encrypt SCI constitutes access to the SCI itself. Keying material is considered SCI when it is removed from its protective packaging or the protective packaging is no longer intact. Access to unencrypted keying material used to protect SCI must be restricted as follows:

a. Keying material designated for encryption of SCI must be issued for use only to personnel indoctrinated for SCI;

b. Personnel required to enter an SCI facility (SCIF) to perform COMSEC duties and thereby have access to (i.e., the opportunity to hear or view) SCI, must be indoctrinated for SCI. Nonindoctrinated personnel may enter the SCIF, when approved by the appropriate authority, if the SCIF is sanitized or the visitor remains under escort by an indoctrinated individual to preclude inadvertent disclosure; and

c. COMSEC managers/custodians, personnel in cryptologistic facilities, and inspection and training personnel handling protectively packaged keying material designated for encryption of SCI are not required to be indoctrinated for SCI. However, these personnel must hold the appropriate clearance in accordance with the classification of the key. Personnel performing destruction of SCI material requiring removal of the protective packaging must be indoctrinated for SCI.

36. Access to Future Editions of Keying Material - Access to future editions of keying material must be limited to COMSEC account personnel until the keying material is issued for use. Storing future key under two-person integrity (TPI), implementing a protective technologies inspection program in accordance with the requirements set forth in SECTION XII of this NSTISSI, or establishing a no-lone zone are acceptable alternatives to this requirement. When key is stored electronically, system or procedural safeguards must be used to limit access to account personnel. Exceptions can be made to these access restrictions in tactical situations when mission requirements dictate.

37. Access to Encrypted Key - Encrypted TOP SECRET Traffic Encryption Key (TEK) must be handled and stored separately from its associated TOPSECRET Key Encryption Key (KEK), or must be held under TPI.

38. No-Lone Zone - A COMSEC no-lone zone must be established under the following circumstances:

a. COMSEC facilities producing hard copy or unencrypted key;

b. COMSEC depots storing or distributing large quantities of keying material (no-lone zones are not required if a protective technologies inspection program meets the requirements set forth in SECTION XII of this NSTISSI and is implemented at user locations supported by the facility);

c. COMSEC equipment contains TOP SECRET key in a hard copy form or the key is set in a mechanical permuter installed in a COMSEC equipment (no-lone zones are not required, if the COMSEC equipment has been modified to preclude single person access by installing locking bars secured by an approved padlock or tamper indicating seals are used in accordance with instructions provided by the NSA Protective Technologies Division); and

d. Although not required, it is recommended, no-lone zones be established at COMSEC facilities charged with providing or supporting essential critical, intelligence, or command and control activities and facilities engaged in the design, development, manufacture, or maintenance of COMSEC equipment.

39. Holdings of Keying Material - User accounts must hold, or have access to, at least one future edition of each short title they issue, regardless of the supersession rate. It is recommended COMSEC accounts at remote areas hold at least a six-month supply of key.

Additional holdings of keying material should be kept as low as operationally feasible to reduce the amount of keying material that must be replaced in the event of a compromise.

40. Shelf Life of Keying Material - Keying material marked CRYPTO is not enclosed in protective packaging must be superseded and destroyed in accordance with NTISSI No. 4004 (reference n.) no later than six years after generation or receipt, unless the NSA [redacted] authorizes a longer retention time.

SECTION IX - STORAGE OF COMSEC MATERIAL

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

41. Security Containers

a. Security containers conforming to federal specifications bear a test certification label stating the security capabilities of the container and lock. Those containers manufactured after 1962 will also be marked "General Services Administration Approved Security Container" on the outside of the top drawer.

d. Repair of a damaged security container must be accomplished by authorized persons appropriately cleared or continuously escorted while so engaged.

e. A security container is considered restored to its original integrity, if all damaged or altered parts are replaced and permanent records document the replaced part.

f. Security containers used to store COMSEC material must be locked or protected by guards or an intrusion detection system, when unattended. They should be located in locked areas during nonworking hours and not accessible to general traffic.

43. Storing SECRET and CONFIDENTIAL Keying Material - SECRET and CONFIDENTIAL keying material must be stored by one of the following methods:

a. Any manner approved for TOP SECRET;

b. A GSA-approved security container;

c. Aboard ships, in a steel filing cabinet having a lockbar secured by a electro-mechanical lock meeting Federal Specification FF-L-2740;

d. In a vault meeting the requirements of reference i.; and

e. In an alarmed or guarded area constructed of strong, solid materials that will deter and detect covert penetration and is equipped with an intrusion detection system.

44. Storing Unclassified Keying Material - Unclassified keying material should be stored in the most secure means available to the user, but at least by a method that will reasonably preclude any chance of theft, sabotage, tampering, viewing, or use by unauthorized personnel.

45. Storage of COMSEC Equipment - COMSEC equipment will be stored as specified below, when it is not under the direct and continuous control of appropriately cleared and authorized personnel. These requirements do not apply to spare or standby COMSEC equipment located within the work area; this type of equipment is considered installed for operation.

a. Keyed COMSEC Equipment - COMSEC equipment containing unencrypted key should not be stored in a keyed condition unless operationally necessary. Keyed equipment must be stored in a manner in accordance with the highest classification of the key and can reasonably be expected to preclude theft or tampering. When equipment containing encrypted key is located in an unmanned space, the CIK must be removed and protected in another location.

b. Unkeyed COMSEC Equipment - Unkeyed classified COMSEC equipment must be stored in the same manner as other U.S. Government material of the same classification. Unkeyed unclassified COMSEC equipment will be stored in a manner at least equal to that approved for the storage of other equivalent high value/sensitive material.

c. CIK - Storage procedures for CIK will normally be addressed in the operational security doctrine for the specific COMSEC equipment/system. Normally, removing and properly safeguarding the CIK permits the equipment to be handled as if it were unkeyed.

46. Storage of Other COMSEC Material - Classified COMSEC material not covered above must be stored in the same manner as other U.S. Government material of the same classification.

SECTION X - COMSEC MANAGERS/CUSTODIANS

47. Appointing COMSEC Managers/Custodians - Personnel appointed as COMSEC managers/custodians must:

a. Be a U.S. citizen (either native-born or naturalized);

b. Possess a final security clearance appropriate for the material to be held in the account (COMSEC managers/custodians having access to TOP SECRET keying material must have a security clearance based on a final background investigation current, within five years). Interim clearances may be approved; however, interim TOP SECRET clearances must be based on a final SECRET clearance. COMSEC managers/custodians, for COMSEC accounts holding unclassified material only, do not require a security clearance or background investigation, but must be trusted, responsible individuals. (Also see paragraph 35 when a COMSEC manager/custodian requires access to SCI.) Contractors and nongovernment personnel clearances must be consistent with reference l.;

c. Be a Commissioned Officer, Warrant Officer, E-6, or higher; government grade of at least GS-7; or equivalent civilian position of responsibility, but must not be assigned other collateral duties that would interfere with or detract from the manager/custodian duties and responsibilities of a COMSEC manager/custodian;

d. Be formally trained in the duties and responsibilities of a COMSEC manager/custodian, as described below (training should be received prior to assignment as a COMSEC manager/custodian or at least within six months after assignment);

e. Not have been previously relieved of COMSEC manager/custodian duties for reasons of negligence or nonperformance of duties; and

f. Have maximum retainability to establish continuity and decrease the possibility of frequent replacement.

48. Duties and Responsibilities - The duties and responsibilities of a COMSEC manager/custodian include, but are not limited to, the following:

a. Ensuring all COMSEC material issued to, or generated and held by, the COMSEC account is safeguarded and controlled in accordance with the requirements of this NSTISSI or the operational security doctrine for the associated COMSEC equipment/system;

b. Maintaining the COMSEC account files and preparing and submitting accounting reports to the COR as required;

c. Ensuring new or additional COMSEC material is properly requisitioned or generated in accordance with department or agency directives;

d. Personally conducting or supervising the inventories required by this NSTISSI;

e. Correcting any deficiencies involving procedures at the account;

f. Ensuring amendments to COMSEC publications are posted in a timely manner and residue pages, resulting from page replacements, are destroyed;

g. Ensuring all mandatory modifications are made to COMSEC equipment;

h. Ensuring COMSEC material is issued only to appropriately cleared or authorized individuals whose duties require it and advising them of their responsibility for properly safeguarding and controlling the COMSEC material in their possession;

i. Maintaining records of all COMSEC material issued to users on hand receipts;

j. Initiating organizational procedures ensuring individuals do not leave the organization without first returning or destroying COMSEC material issued to them on a hand receipt;

k. Ensuring routine destruction of COMSEC material is accomplished in accordance with the requirements of reference n.;

l. Ensuring Standard Operating Procedure (SOP), emergency protection, or destruction plans prepared in accordance with the requirements of reference n., exist at all COMSEC facilities served by the COMSEC account;

m. Ensuring COMSEC material handled within the CMCS is properly packaged for transportation, and all received packages are examined for evidence of tampering (All reports of tampering must be reported in accordance with the requirements of reference h);

n. Ensuring protective technologies are inspected in accordance with instructions published by the NSA Protective Technologies Division (All reports of tampering must be reported in accordance with the requirements of reference h.);

o. Ensuring COMSEC material received or transferred by the account agrees with material listed on the accompanying transfer report;

p. Ensuring COMSEC incidents are reported in accordance with the requirements of reference h.;

q. Making transportation arrangements and ensuring only authorized means are used for transporting COMSEC material;

r. Ensuring the COMSEC account holds only COMSEC mission essential material;

s. Training users in proper procedures for safeguarding and controlling COMSEC material;

t. Working with the COMSEC user to ensure there is a continuing requirement for specific key or, if no requirement, recommending to the controlling authority that the account be dropped from distribution of that specific key; and

u. Ensuring the account is properly transferred prior to departing an assignment.

49. Assistant COMSEC Managers/Custodians - The assistant COMSEC manager/ custodian must be aware of the day-to-day operations of the COMSEC account and must be able to perform all required duties during any absence of the primary COMSEC manager/ custodian. One assistant COMSEC manager/custodian will be appointed for each COMSEC account. Additional assistants may be appointed, as necessary, to maintain continuity of operations subject to the approval of the COR.

a. An assistant COMSEC manager/custodian must meet the same citizenship and security clearance requirements as the primary. Personnel appointed as assistant COMSEC managers/custodians should be experienced in the COMSEC field and must

hold military grade of at least E-5, government grade of at least GS-5, or equivalent civilian position of responsibility.

b. Assistant COMSEC managers/custodians should be formally trained in their duties and responsibilities. Training should be received within six months after assignment.

50. Other Account Personnel - COMSEC managers/custodians may use other personnel (e.g., COMSEC clerks or COMSEC accountants) to assist in the day-to-day administration and maintenance of accounting records. However, such personnel may not assume responsibility for COMSEC material held in a COMSEC account, other than personal responsibility to safeguard the COMSEC material.

51. Temporary Scheduled Absence of COMSEC Managers/Custodians - During a temporary scheduled absence of the COMSEC manager/custodian, the assistant will assume all duties. An absence of the COMSEC manager/custodian for a period greater than 60 days should be considered an extended absence, and a new COMSEC manager/custodian should be appointed. (Waiver exceptions for an additional 30 days will be considered in the event of operational necessity.)

SECTION XI- ACCOUNTING, INVENTORY, AND AUDITS

52. Each COR shall:

a. Establish and close COMSEC accounts;

b. Maintain a record of all COMSEC material issued to COMSEC accounts under its cognizance and update records by conducting routine audits;

c. Monitor for receipt of in-transit COMSEC material;

d. Establish or approve procedures for reporting receipt and transfers of COMSEC material;

e. Establish or approve accounting procedures for accounts under its cognizance;

f. Ensure compliance with accountability requirements for COMSEC material;

g. Establish inventory and audit procedures for COMSEC accounts;

h. Ensure audits are conducted in accordance with paragraph 67 of this NSTISSI;

i. Provide disposition instructions on superseded, excess, and obsolete COMSEC material; and

j. Provide COMSEC managers/custodians relief from accountability when necessary.

53. Reporting and Accounting for COMSEC Material - COMSEC material, other than what is generated under the provisions of doctrine, Field Generation and Over-The-Air

Distribution of COMSEC Key in Support of Tactical Operations and Exercises (NAG-16, dated Aug 96), is assigned to an accounting legend code (ALC) depending upon classification, purpose, and inventory requirements. ALCs 1, 2, and 4 are assigned to material that must be physically inventoried by the COMSEC manager/custodian. ALCs 6 and 7 are assigned to material in electronic form that cannot be physically inventoried but must be electronically inventoried by EKMS-certified components. EKMS may be used by the COMSEC manager/custodian to maintain disposition records and support reporting requirements for all classes of material. Tactical key generated under the provisions of NAG-16 is not assigned an ALC. Departments and agencies may not reassign material a different ALC without prior approval from NSA, except when such reassignment is an intrinsic part of an electronic key distribution process performed by EKMS.

54. ALC 1, Continuously Accountable by an Accounting Number to a COR - The following material is continuously accountable and will be assigned ALC 1:

a. All hard copy and magnetic keying material marked CRYPTO (except for machine off-line COMSEC aids, operations codes, and authentication systems that are classified CONFIDENTIAL or below);

b. All classified equipment and CCI identified by an external nameplate containing the equipment nomenclature and serial number;

c. Classified cryptographic software and firmware that are the functional equivalents of, or emulate, COMSEC equipment operations and cryptography; and

d. Classified full and depot maintenance manuals and other classified TSEC-nomenclature publications and amendments thereto, except as specified in paragraph 58.d. of this NSTISSI.

55. Accounting for ALC 1 Material

a. General - A report will be submitted to the COR upon receipt and all subsequent transfers of ALC 1 material. The COR will maintain a record of all ALC 1 material charged to a COMSEC account. All transactions involving material assigned ALC 1 including, but not limited to, issue for use and destruction will be recorded on a local disposition record. The local disposition records will be reported to the COR and retained by the COMSEC manager/custodian until the next audit or other COR-approved COMSEC inspection.

b. FIREFLY-based Systems - For FIREFLY-based systems only, additional reports will be submitted to the appropriate COR when operational fill devices are loaded into the equipment and seed or operational fill devices are locally zeroized.

56. ALC 2, Continuously Accountable by Quantity to a COR - The following material is continuously accountable by quantity and will be assigned ALC 2:

a. Spare (i.e., intended for installation, but not actually installed) classified and CCI components (e.g., microcircuits, printed circuit boards, permuters, and subassemblies) intended for installation in equipment accountable by serial number;

b. Noncryptographic classified devices performing critical key processing ancillary functions (e.g., fill devices); and

c. Keying devices when unkeyed.

57. Accounting for ALC 2 Material - A report will be submitted to the COR upon receipt, and any subsequent transfers of ALC 2 material changing the total quantity held by a COMSEC account. The COR will maintain a record of all ALC 2 material charged to a COMSEC account. All transactions involving ALC 2 material will be recorded on a local disposition record. The local disposition record will be retained by the COMSEC manager/custodian until the next audit or other COR-approved COMSEC inspection.

58. ALC 4, Report of Initial Receipt Required - The following material will be assigned ALC 4:

a. All hard copy and magnetic keying material not marked CRYPTO;

b. Call sign systems (e.g., CEOI/JCEOI/SOI);

c. Unclassified hardware, software, or firmware (i.e., (programmable read-only memory (PROM) or other unclassified chips except those marked CRYPTO); and

d. Classified limited maintenance manuals and all unclassified TSEC-nomenclature publications and their amendments.

59. Accounting for ALC 4 Material - This material will be handled within the CMCS, but only the first recipient must report receipt to the COR. All subsequent transactions will be recorded on local disposition records which will be retained in accordance with the instructions of the COR. ALC 4 material will be safeguarded in accordance with its classification.

60. ALC 6, Continuously Accountable to a COR by Means of the EKMS - The following EKMS-generated and managed electronic key and other electronic data will be assigned ALC 6:

a. Any electronic key material requiring continuous, central accountability from a security or operational standpoint, as determined by the controlling authority and specific system doctrine, where applicable. Some examples of keys designated ALC 6 are:

(1) Electronic keys intended to protect information having long-term intelligence value, as determined by the controlling authority (e.g., TOP SECRET/SCI);

(2) Electronic keys used to protect other keys (e.g., KEK) when such keys are widely distributed, or when used for encryption of large numbers of keys; and

(3) Electronic keys used for joint interoperability, when such keys are widely distributed.

b. Electronic keys marked CRYPTO used to generate other electronic keys (e.g., Key Production Keys, FIREFLY keys);

c. All classified software, firmware, or equivalent data in electronic form performing cryptographic operations; and

d. Additional guidance introducing transition to the EKMS and doctrinal requirements for the handling and accounting of electronic key are contained in ANNEXes C and D.

61. Accounting for ALC 6 Material - A report will be submitted to the COR upon the generation, receipt, transfer, and/or destruction of ALC 6 material. The COR will maintain a

record of all ALC 6 material charged to a COMSEC account. All transactions involving ALC 6 material including, but not limited to, issue for use and destruction (zeroization) will be recorded in a local disposition record. The local disposition records will be retained by the COMSEC manager/custodian until the next audit or other COR-approved COMSEC inspection.

62. ALC 7, Continuous Local Accountability within the EKMS - EKMS-generated and managed electronic key, and other electronic data not covered by ALC 6 will be assigned as ALC 7.

63. Accounting for ALC 7 Material - Each recipient of ALC 7 key will give a receipt to the EKMS element that sent the key. Elements generating ALC 7 key must maintain local records documenting the generation of key. All holders of ALC 7 material must maintain local disposition records permitting traceability to support compromise recovery and audits. As a minimum these records shall identify all transactions involving subsequent transfer, issue, fill, and destruction of the material, as applicable.

64. Accounting for COMSEC Material at User Locations

a. Holdings of keying material at user locations should be kept to the minimum amount necessary to meet operational requirements. In situations where responsibility for keying material is transferred from shift-to-shift, shift supervisors are responsible for ensuring that all keying material receipted for is intact and for inspecting protective technologies for evidence of penetration or substitution in accordance with instructions published by the NSA Protective Technologies Division.

b. At user locations, keying material marked CRYPTO will be inventoried by serial number on days when the security container is opened (containers do not need to be opened for inventory purposes only). The inventory will be made a matter of record whenever heads of appropriate departments or agencies believe it appropriate. Other COMSEC material will be inventoried in accordance with the instructions of the COR.

c. Disposition records must be maintained for all keying material marked CRYPTO and for keyed fill devices so personal responsibility can be traced in the event of a compromise. (These disposition records must be maintained for a period of three years.) The disposition record must identify the material, the date of issue, the person to whom the material was issued, and the date of destruction. When TOP SECRET key is issued under TPI, both recipients must be indicated. Hard copy records must be initialed or signed by recipient(s) and destroying and witnessing personnel. Electronic records may be kept in lieu of hard copy records, if the record can establish personal responsibility and is authorized by the COR. When keying material is issued to transient personnel, the issuing COMSEC manager/custodian is relieved of accountability by so annotating the hand receipt.

d. Keying material not marked CRYPTO will be accounted for in the same manner as other U.S. Government material of the same classification.

e. COMSEC material will be page checked in accordance with its handling instructions. Users are encouraged to periodically ensure pages of technical manuals are intact.

65. Transferring COMSEC Material - Keying material will not be transferred between COMSEC accounts without controlling authority approval. Transfers of COMSEC material will be documented in accordance with the instructions of the COR. COMSEC managers/ custodians transferring material must ensure they receive a receipt. Individual hard copy key

settings must not be transferred between COMSEC accounts except in cases of operational necessity.

66. Inventory Requirements - ALCs 1, 2, and 4 COMSEC material controlled within the CMCS must be physically inventoried by the COMSEC manager/custodian and an appropriately cleared witness, preferably the assistant manager/custodian. ALCs 6 and 7 COMSEC material must be electronically inventoried by EKMS-certified components under the control of the COMSEC manager/custodian. Inventories must be performed at the periodic intervals specified below:

a. User Account Periodic Inventory - Classified material marked CRYPTO must be inventoried by the COMSEC manager/custodian semiannually; all other material must be inventoried annually. This inventory must be conducted with an appropriately cleared individual, preferably the assistant COMSEC manager/custodian, serving as witness. Material held at remote sites need not be physically sighted, but a new hand receipt must be issued semiannually. Inventory reports will be signed by the COMSEC manager/custodian and the witness; the report will be forwarded to the COR or filed in accordance with department or agency directives. Cryptographic, personnel, and physical incidents detected during an inventory must be reported as outlined in reference h. Inventory paperwork discrepancies that cannot be resolved within six months, must also be reported as possible COMSEC incidents in accordance with reference h.:

NOTE: If the audit required in paragraph 67, below, includes a completed inventory, it may replace one of the semiannual inventories.

b. COMSEC Depot and Cryptologistic Facility Periodic Inventory - Because of the volume of COMSEC material stored at these facilities, COMSEC managers/custodians may satisfy the periodic inventory requirement by any means ensuring all classified keying material marked CRYPTO is inventoried semiannually and all other material is inventoried annually;

c. Change of COMSEC Manager/Custodian Inventory - An inventory of all COMSEC material must be taken at each account prior to changing COMSEC managers/ custodians. This inventory should be conducted jointly by the incoming COMSEC manager/ custodian and the outgoing, who will serve as witness. At COMSEC depot and logistics support facility accounts, inventory teams may assist in conducting the inventory under the supervision of the COMSEC manager/custodian. Results of the inventory must be reported in accordance with department or agency directives; and

d. Unauthorized Absence or Sudden Permanent Departure of the COMSEC Manager/Custodian - An inventory of all COMSEC material must immediately be conducted upon the unauthorized absence (as determined by department or agency directives) or sudden permanent departure of the COMSEC manager/custodian. The assistant COMSEC manager/ custodian, with an appropriately cleared witness, will conduct this inventory and will report in accordance with department or agency directives. The report must be annotated to reflect the circumstances involved and will be signed by both the assistant COMSEC manager/custodian and the witness. A new COMSEC manager/custodian will then be formally appointed. If either the witness or the assistant COMSEC manager/custodian is subsequently appointed COMSEC manager/custodian, the COR may delete the requirement for a change of COMSEC manager/ custodian inventory.

67. COMSEC Audits - Each COR shall ensure an audit of each of its COMSEC accounts is conducted on an aperiodic event-driven basis. Such audits shall be conducted to ensure COMSEC accounts are complying with applicable requirements governing

accountability, handling, and safeguarding of COMSEC material. The COR, or the COMSEC authority designated by a department or agency, shall determine the frequency of these audits, which should be based on sound risk management principles. Normally a COMSEC account should not be audited at intervals less frequently than 12 successive months between audits. However, more frequent audits may be warranted, if an account repeatedly shows discrepancies in its accounting, handling, or control procedures. Audits shall be conducted by a representative of either the COR or the department or agency COMSEC authority, as appropriate. To the maximum extent possible, the audit should be conducted in the presence of the COMSEC manager/custodian. In addition to an administrative review of procedures, the COMSEC account audit should also include a 100 percent sighting of all keying material marked CRYPTO. At facilities producing COMSEC material, the audit shall include a review of in-process accounting procedures, as well as, accountable material in the manufacturing process.

68. Exceptions - Sealed packages or containers of COMSEC material received at COMSEC depots should not be opened solely for inventory purposes. If the packages must be opened for any reason, the contents must be inventoried. Packages showing evidence of tampering or penetration will be reported in accordance with the requirements of reference h. and will not be opened until authorization is received from NSA.

SECTION XII - THE PROTECTIVE TECHNOLOGIES INSPECTION PROGRAM

69. NSA provides state-of-the-art tamper-revealing products for information processing equipment and keying material. However, the level of protection obtainable from these products depends almost entirely upon the inspection and control programs conducted by users. To ensure the integrity of protective technologies, heads of appropriate departments and agencies must:

a. Ensure personnel who routinely handle or use protectively packaged keying material or tamper-sealed information processing equipment are trained in the procedures for inspection and disposal of used protective technologies;

b. Establish procedures requiring inspection of protected items upon receipt, during each inventory, and prior to opening or removal of protective technologies when required for use or maintenance in accordance with instructions published by the NSA Protective Technologies Division;

c. Ensure COMSEC inspections and audits performed at user and user account locations include inspections of selected protective technologies, including the use of classified and other special inspection techniques made available by NSA to auditing and inspection offices (where feasible, implement a program of inspections conducted at random intervals without advance notification. As a general guideline, at least 10 percent of the total number of applicable locations under the department or agency's control should be subjected to unscheduled inspections annually); and

d. Inform NSA of any suspect or possibly compromised items and forward this information in accordance with instructions from the NSA Protective Technologies Division, as operational necessity permits.

70. In addition to the foregoing, departments and agencies implementing a program of unscheduled inspections of protected TOP SECRET material at COMSEC account locations (including a random selection of at least 25 percent of such locations per year), may waive TPI for keying material while it is contained inside intact protective packaging.

71. The NSA Protective Technologies Division is available to assist departments and agencies in designing alternative inspection programs and processes to fit particular operational environments.

SECTION XIII - ISSUING AND USING COMSEC MATERIAL

72. General - Keying material must be issued only after it has been determined the recipient has been granted access in accordance with the requirements of this NSTISSI and can properly safeguard and control the material. After the material has been properly issued for use in accordance with the requirements of paragraph 64.c., the issuing COMSEC manager/ custodian is relieved of his/ her personal responsibility for the security of the material but must still account for the material. The recipient of COMSEC material is personally responsible for its use and protection. Under no circumstances will the recipient re-issue the material to another individual without the consent of the COMSEC manager/custodian. Key must be issued as close to its effective time as practical; however, specific time frames for issuing key are not prescribed due to divergent operational requirements.

73. High Risk of Capture - Only mission essential COMSEC material may be held in environments where there is a high risk of capture by an adversary. In high risk environments, key will be issued in electronic form when possible. Communications nets should be kept as small as possible.

74. Determining High Risk of Capture Environments - ANNEX E to this NSTISSI provides a guide for determining whether or not a particular environment presents a high risk of capture. Responsible officials should select one situation from each category and add the points. Any scenario totaling 15 points or higher is considered high risk; however, the guide is not all inclusive. Responsible officials may declare a high risk environment whenever circumstances warrant. In a training environment, the risk assessment should be based on the training scenario rather than actual environment.

75. Issuing Keying Material in Tactical Situations - TPI handling is not required in tactical situations. The amount of key that may be issued in tactical situations is not limited: keying material will be issued in sufficient quantities to support mission requirements. Keying material can be issued in either hard copy or electronic form depending on the risk as determined by the local commander. If key is issued in electronic form, any multiple key storage capacity of the equipment should be used. If equipment does not have multiple fill capacity (or has insufficient capacity), approved fill, key transfer, or storage devices should be issued. If hard copy keying material is issued, extracts may be issued when only a few settings are required; otherwise, the entire edition or editions should be issued based on a risk assessment and careful consideration of the logistics problems associated with emergency resupply due to compromise of hard copy key.

a. The premature exposure of keying material is permitted for units/elements deploying under real world crisis/contingency scenarios. These units/elements may down-load the current edition plus the minimum amount of keying material necessary for the crisis scenario, up to a maximum of an additional 90 days keying material, into a DTD. (Fill devices such as the KYK-13 and KYK-15 may not be used for this purpose). Requests for extensions in excess of the current edition plus 90 days must be directed to the NSA Information Systems Security Policy and Doctrine Division for approval.

b. Tactical units deploying in other than crisis/contingency situations should limit their number of segments loaded into the DTD to those required for the mission. Loading of the DTD from punched tape should be limited to those segments required while the unit is absent from normal COMSEC support.

c. Controlling authority will notify the COMSEC custodian, in writing, of the material to be down-loaded.

d. When duplicate key is readily available, the exposed hard copy key segment(s) should be destroyed immediately after loading into the DTD. If there is no duplicate key, place the exposed segment, along with a copy of the approval from the controlling authority, in an envelope. Seal and store the envelope in the plastic bag containing the associated key tape canister.

e. The DTD should have the CIK removed any time the DTD is not in use.

76. Unattended COMSEC Equipment - Requirements for protecting COMSEC equipment in unattended telecommunications facilities are contained in paragraph 29.a. of this NSTISSI. In other types of facilities, keyed COMSEC equipment may be left unattended while operating or in a standby mode if, in the opinion of the responsible authority, either the equipment or the information being processed is protected sufficiently to reasonably preclude theft, sabotage, tampering, or unauthorized access. When COMSEC equipment is securing a computer network, the network or system administrator must first approve the procedure. The following guidelines apply:

a. If the information protected by the keyed equipment can be printed or read out in the area holding the equipment, the area should be approved for open storage of information classified up to the level of the key; and

b. If the information protected by the keyed equipment cannot be printed or read out in the area holding the equipment, the keyed equipment may be protected by lockbars secured by an electro-mechanical lock meeting Federal Specification FF-L-2740 or may be secured in a container having been approved by NSA for closed-door operation, or the area holding the equipment may be secured by an electro-mechanical lock meeting Federal Specification FF-L-2740.

77. Issuing Keying Material for Use Within Fixed Facilities - In fixed facilities, the primary threat to keying material is surreptitious copying (either physically or by electronic duplication) by a hostile cognizant agent. The following guidance is provided to counter that threat:

a. Keying material should remain inside its protective packaging until it is issued for use. Prior to the withdrawal of key tape or the opening of sealed packaging, the protective packaging must be examined for indications of possible tampering in accordance with instructions published by the NSA Protective Technologies Division;

b. Protectively packaged key may be issued for use as extracts or entire editions in accordance with the instructions of the controlling authority. When users require more than one key setting, protectively packaged keying material should be issued as entire editions, whenever possible, since removing key from its protective packaging defeats the purpose of the protective packaging and exposes the key to surreptitious copying. If key is issued as extracts, the extracts must be enclosed in an opaque envelope sealed in a way to reveal attempts at penetration, (e.g., initialed across the flap or sealed with logo type laminating material);

c. Common fill devices such as the KYK-13 and KYX-15 that store key in unencrypted form and provide no record of transaction must not be used for long-term storage of key. Key can be held in this type of fill device no longer than 12 hours from the time it is loaded into the terminal equipment or 12 hours after the end of the applicable cryptoperiod.

except in cases of operational necessity. This type of fill device must be kept under TPI whenever it holds TOP SECRET key and must be marked to show the highest classification of key contained inside;

d. Fill devices such as the AN/CYZ-10 (DTD) that store key in encrypted form will be used in accordance with their operational security doctrine;

e. Magnetic storage media containing unencrypted electronic key must be returned to secure storage after the key or associated data has been loaded into the terminal equipment;

f. Removable magnetic storage media holding key must be marked to show the highest classification of key held and carry the CRYPTO caveat, if applicable;

g. Magnetic storage media (e.g., tapes, floppy disks, hard disks) having held keying material marked CRYPTO may be reused but must retain the highest classification of any key previously held. The CRYPTO caveat may be removed, if the media is degaussed using an approved device or is overwritten using an NSA-approved procedure. (Approved devices and procedures are contained in NSA/CSS Manual 130-2, Media Declassification and Destruction Manual and approved degaussers are listed in the NSA INFOSEC Products and Services Catalogue); and

h. At the user level, encrypted TEK and its associated KEK must be handled separately or under TPI.

78. Using COMSEC Material

a. Keying material must be used only for its intended purpose and only on the equipment for which it was produced. Generic key will be used only as directed by the controlling authority. Keying material must not be used on anything other than the designated equipment without the approval of the NSA Information Systems Security Policy and Doctrine Division.

b. If operations must be interrupted for on-the-air testing, the operational key may be used for the test.

c. Only NSA-developed or endorsed COMSEC equipment, keying material, and techniques may be used by or on behalf of U.S. Government departments and agencies to protect national security information. COMSEC material must be used only for its intended purpose.

d. Computer systems producing or storing unencrypted key in electronic form must be either stand-alone systems or systems in a network environment having been evaluated and endorsed by NSA.

e. In cases of operational necessity, keying material may be used to encrypt information of one higher level of classification (e.g., CONFIDENTIAL keying material may be used to encrypt SECRET information). In emergency situations, keying material that has been provided the greatest security should be used to protect classified information, regardless of its classification. The only exception to these two provisions is that unclassified key not marked CRYPTO will not be used to protect any classified information.

79. Cryptoperiod Extensions - Cryptonet members can extend cryptoperiods for two hours without controlling authority authorization when necessary to complete a transmission or conversation. Cryptonet members are not required to report these extensions. Longer

cryptoperiod extensions must be approved by the controlling authority in accordance with the instructions and limitations of NSTISSI No. 4006 (reference o.).

80. Loading TOP SECRET Keying Material - In static environments, TPI handling procedures must always be applied to keying operations. Loss of TPI must be reported as a COMSEC incident. If heads of appropriate departments and agencies approve alternative arrangements to TPI, the controlling authority will be notified. TPI handling is not required in tactical situations.

81. QUADRANT Inspection - COMSEC equipment must be inspected for unauthorized internal access and tampering by NSA or the user's department or agency whenever COMSEC equipment:

a. Remains in a facility during alteration, renovation, or the performance of maintenance by personnel not certified in accordance with NSTISSI No. 4000 (reference p.);

b. Is recovered from a facility that has been abandoned or captured and occupied by other than authorized personnel; and

c. Is lost in shipment and is later recovered.

82. COMSEC Publications - Operating instructions should be held in the same area where COMSEC equipment is operated. Maintenance manuals should be issued only to those locations where maintenance personnel are assigned.

SECTION XIV - TRANSPORTATION OF COMSEC MATERIAL

83. General - Throughout this NSTISSI the term (or variation of the term) "transportation" is used when no distinction is made as to the method of conveyance; "shipment" is used to denote a method of conveyance that does not allow personal custody or control of the material while in transit (e.g., Defense Courier Service (DCS), State Department Courier Service, U.S. Postal Service, Protective Security Service); and "courier" and "carry" are used interchangeably to denote a method of conveyance allowing personal custody or control of the material while in transit.

NOTE: For purposes of this NSTISSI, the term "courier" refers to a person who receives material at point A and delivers it to point B. The term does not include tactical users who must carry material from point A to point B for their own operational use.

84. Preparation for Transportation

a. All keying material and other classified COMSEC material must be double-wrapped or otherwise encased in two opaque containers and securely sealed prior to transportation. Material used for packaging must be strong and durable enough to provide protection while in transit, prevent items from breaking through the container, and facilitate the detection of any tampering with the container. The outer wrapper must not provide any indication the package contains classified material or keying material.

b. Unclassified COMSEC material other than key should be appropriately wrapped to detect tampering or penetration and protect against damage.

c. When material is carried, a briefcase, pouch, or box is an appropriate outer wrapper.

d. If the classified material is internal to a piece of equipment, the equipment shell or body may be considered as the inner wrapper. Specialized shipping containers for equipment may be considered the outer wrapper or cover; however, any classification or COMSEC markings must be taped over.

85. Transportation of Keying Material - Operational keying material cannot be shipped in the same container with its associated equipment unless the physical configuration of the equipment makes segregation of the keying material impossible; however, unclassified maintenance key may be shipped in the same container as the associated equipment. Uncleared commercial carrier services will not be used to ship classified keying material marked CRYPTO.

a. TOP SECRET and SECRET - All TOP SECRET and SECRET keying material marked CRYPTO must be transported by one of the following methods:

(1) DCS;

(2) State Department Courier Service; or

(3) Formally designated and appropriately cleared department, agency, or contractor couriers.

b. CONFIDENTIAL - CONFIDENTIAL keying material marked CRYPTO must be transported by one of the following methods:

(1) Any method approved for TOP SECRET/SECRET;

(2) U.S. Postal Service Registered Mail, provided the material does not pass through a foreign postal system or any foreign inspection; or

(3) Protective Security Service (PSS). (PSS is provided by commercial carriers who have security clearances granted by the Defense Investigative Service. These commercial carriers are cleared only to the SECRET level.)

c. Unclassified - Unclassified keying material marked CRYPTO must be transported by one of the following methods:

(1) Any method approved for TOP SECRET/SECRET/ CONFIDENTIAL; and

(2) For shipments within the limits of the U.S., its territories, and possessions, an uncleared carrier, providing that the carrier meets the following criteria:

(a) Must be a firm incorporated in the U.S.;

(b) Must provide continuous accountability of shipments equivalent to the tracking available through the U.S. Postal Service Registered Mail; and

(c) A distant-end signature receipt is provided.

86. Transportation of COMSEC Equipment - COMSEC equipment may not be shipped in a keyed condition unless the physical configuration of the equipment makes segregation of the keying material impossible; however, couriers may hand carry keyed COMSEC equipment.

a. SECRET COMSEC equipment and all key production equipment (e.g., KOK-13, KOK-22, KG-83) must be transported by one of the following methods:

(1) DCS;

(2) State Department Courier Service;

(3) Formally designated and appropriately cleared department, agency, or contractor couriers; or

(4) Cleared commercial carrier using PSS. (PSS is provided by commercial carriers who have security clearances granted by the Defense Investigative Service. These commercial carriers are cleared only to the SECRET level.)

b. CONFIDENTIAL COMSEC equipment (except key production equipment) may be transported by one of the following methods:

(1) Any method approved for SECRET;

(2) U.S. military or military-contractor air service (e.g., Air Force Mobility Command (AMC), LOGAIR, QUICKTRANS); or

(3) U.S. Postal Service Registered Mail, provided the material does not pass through a foreign postal system or any foreign inspection.

c. Requirements for transporting CCI are set forth in NSTISSI No. 4001 (reference g.).

d. UNCLASSIFIED COMSEC equipment may be transported by any method approved for the shipment of other equivalent high value/sensitive material.

87. Transportation of Other COMSEC Material - COMSEC material not covered in paragraph 85 and 86 of this NSTISSI may be transported as any other material of the same classification.

88. Transportation of Cryptographic Algorithms or Logic - Cryptographic algorithms and logic will not be transported without the approval of the NSA program manager for the associated equipment. All cryptographic algorithms or logic will be transported by one of the following methods:

a. DCS;

b. State Department Courier Service; or

c. Formally designated and appropriately cleared department, agency, or contractor couriers.

89. Limitations on Shipments

a. When shipping keying material marked CRYPTO, packages should contain as few editions as possible of each short title. The goal is to minimize the number of editions that must be replaced if the shipment is compromised. It is recommended a package

contain no more than four editions of material that are superseded quarterly or more frequently, or two editions if the material is superseded semiannually or less frequently. If large numbers of editions must be shipped, the material should be split into several packages and entered into courier services in staggered shipments, that are not likely to be combined by the courier service. There is no restriction on the number of short titles that can be enclosed in each package or the number of copies of each edition.

b. Encrypted TEK and its associated KEK must be shipped in separate packages.

90. Use of Commercial Airline by Couriers - Any commercial airline can be used to carry COMSEC material within the continental U.S. Non-U.S. flag airlines may be used to carry COMSEC material outside the continental U.S., if the courier's department or agency approves. Only limited quantities of future keying material (editions or settings) should be carried outside the U.S. Sufficient time should be available to supersede the material should it be compromised (at least three duty days should remain before implementation). Whenever possible, couriers should use nonstop flights. If nonstop flights are not available, layovers for connecting flights should be kept to a minimum.

91. Use of Private Conveyances - Private or corporate-owned conveyances can be used to carry COMSEC material. The recipient organization should be notified of the itinerary and estimated time of arrival, so appropriate steps may be taken if the courier does not arrive on time.

92. Couriers

a. Couriers for COMSEC material must be specifically designated in writing by the authorizing official. It is the responsibility of the authorizing official to ensure all couriers are properly cleared, trustworthy, and briefed on their responsibilities for safeguarding the material entrusted to them. Couriers must be provided instructions covering emergency situations including loss or other compromise of the material they are carrying. Couriers traveling outside the continental U.S. must be provided the telephone number of the nearest U.S. Embassy or Consulate in every country through which they will travel. The identification card and letter of authorization requirements contained in Federal Aviation Administration Advisory Circular 108-3, Screening of Persons Carrying U.S. Classified Material (available from the U.S. Government Printing Office) must be complied with.

b. Couriers may hand carry keyed COMSEC equipment. Couriers may hand carry encrypted TEK and associated KEK.

93. Courier Responsibilities

a. When carrying keying material, couriers must maintain constant personal custody of all keying material entrusted to them.

b. When carrying COMSEC material other than keying material, couriers are responsible for ensuring the safety of the material at all times. Couriers may place bulky material in a locked compartment using last in-first out procedures, if the carrier restricts access to the lock combination or key to authorized employees. Couriers must ensure the material is given the maximum protection possible during transit and not left unattended on loading docks, in cargo storage areas, baggage areas, etc.

c. [redacted]

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

d. Couriers need not be armed unless local conditions deem it advisable by the appointing official.

94. Security Requirements for Airdrop - COMSEC material should not be flown over hostile territory, unless, it is operationally necessary. When COMSEC material must be transported or airdropped over hostile territory in support of tactical operations, the following safeguards should be observed:

a. COMSEC material must not be airdropped, unless, there is a high probability of the material's immediate recovery by authorized personnel;

b. Airdropped COMSEC material must be under the control of a properly cleared individual until the material leaves the aircraft;

c. Vehicles or shelters, in which COMSEC equipment is installed, may be transported by helicopter using sling-loading techniques; and

d. COMSEC keying material and publications must not be sling-loaded, but may be carried inside the same helicopter that is transporting the equipment.

95. Action Upon Receipt - Packages must be inspected for damage or evidence of penetration immediately upon receipt in accordance with the instructions published by the NSA Protective Technologies Division.

96. Emergency Transmission of Key - Under emergency circumstances, printed key settings may be transmitted by any cryptosystem providing end-to-end encryption equal to the classification of the transmitted key (e.g., the Automatic Digital Network [AUTODIN] system, secure facsimile, or secure telephone). The key must not appear in plain text anywhere in the communications path. Printed key settings can also be encrypted by auto-manual or one-time pad system and transmitted over a system that is secured at a lower level than the encrypted key.

SECTION XV - PROTECTING PASSWORDS AND LOCK COMBINATIONS

97. Passwords - Passwords for computers that contain or are used to protect COMSEC information must be selected and protected in accordance with the guidelines contained in the DoD Password Management Guideline, CSC-STD-002-85. The DoD Password Management Guideline is available from the U.S. National Distribution Authority (USNDA), 1472 Dorsey Rd., Hanover, MD 21076.

98. Changing Combinations - A lock combination may only be changed by a cleared individual having a need-to-know for the information safeguarded by the lock. Combinations must be changed:

a. When the lock is initially placed in use. (The manufacturer's preset combination may not be used.);

b. When any person having authorized knowledge of the combination no longer requires such knowledge (e.g., through transfer or loss of clearance);

c. When the possibility exists that the combination has been subjected to compromise;

d. When the lock is taken out of service. (Built-in locks must be set to the standard combination 50-25-50, and padlocks must be set to the standard combination 10-20-30);

e. When any repair work has been performed on the combination lock; and

f. At least once every two years or sooner as dictated by the above events.

99. Classification of Combinations - Lock combinations and passwords must be assigned the highest classification of any information protected by the lock. For a security container, this is the highest classification of the information held in the container; for a facility door, it is the highest classification of the information held in the facility, including the information stored in the containers.

100. Access to Combinations - Access to the combination of a lock used to protect COMSEC material must be limited to individuals who are authorized access to the material in accordance with this NSTISSI. Where a container is used to store future or superseded editions of key, access to the combination must be restricted to COMSEC account personnel.

101. Selection of Combinations - Each lock should have a combination composed of randomly selected numbers based on the manufacturer's specifications. That combination must not deliberately duplicate a combination selected for another lock within the facility and must not be composed of successive numbers in a systematic or predictable sequence (e.g., birthdays, social security numbers, and telephone numbers).

102. Record of Combinations

a. To provide for ready access to secured material in emergencies, a central record of lock combinations should be maintained in a security container approved for storage of the highest classified combination. The combination to the container holding the central record of lock combinations must be restricted to persons with proper clearance and need-to-know.

b. If a container is used for TPI storage, it is strongly recommended both combinations be protectively packaged separately and held at separate locations. (It is understood that there may be situations where a single individual, such as the facility security officer, will have access to both combinations securing the material.) If the combinations to a container used for TPI storage are not protectively packaged, the combinations must be stored at separate locations.

c. It is specifically prohibited for individuals to record and carry, or store insecurely for personal convenience, the combinations to facilities or containers where COMSEC material is stored. Records of such combinations may not be stored in electronic form in a computer or at unattended or contingency facilities.

103. Protective Packaging of Lock Combinations - Lock combinations should be packaged and sealed in special commercially available tamper-indicating envelopes (e.g., bank bags) recommended by the NSA Protective Technologies Division. The protective packaging should be inspected at least monthly.

104. Emergency Transmission of Combinations - Under emergency circumstances, lock combinations may be transmitted by any cryptosystem providing end-to-end encryption equal to the classification of the lock combination (e.g., the AUTODIN system, secure facsimile, or secure telephone). The combination must not appear in plain text anywhere in the communications path. Lock combinations can also be encrypted by auto-manual or one-time pad system and transmitted over a system secured at a lower level than the encrypted key.

SECTION XVI - ALTERATION AND REPRODUCTION

105. Unauthorized Alterations or Modifications of COMSEC Material

a. It is expressly forbidden to apply any type of label to protective packaging such as canisters, marbleized wrapping and logo tape, as it will divert attention from actual or attempted penetration of the material. Grease pencil and markers may be used if it is absolutely necessary to mark a surface.

b. No modification, change, or alteration of any kind may be made to any COMSEC material without the prior approval of NSA.

c. The fabrication of COMSEC equipment by the means of cannibalization from other equipment held in stock is prohibited.

106. Reproduction - COMSEC material is considered to be reproduced when it has been duplicated in like form (e.g., creating a back-up copy of a disk) or converted to hard copy form for equipment fill (e.g., extracting a key file from a disk and storing it on a key storage device). Converting hard copy key to electronic form for immediate equipment fill is not considered reproduction. Reproduced material must be documented and controlled in accordance with department or agency directives.

a. Manual cryptosystems (codes, authenticators, and call signs) not nuclear command and control material may be reproduced as necessary to meet operational requirements, unless specifically prohibited in the associated handling instructions. Controlling authority approval is not required; however, controlling authorities should be notified as soon as it is operationally feasible. This material can only be issued to authorized users.

b. Keying material for machine cryptosystems will not be reproduced without the consent of the controlling authority. If controlling authority approval cannot be obtained in time to meet operational requirements, or if a controlling authority is not designated, the local commander can authorize reproduction. The controlling authority must be notified at the earliest opportunity.

c. [redacted]

d. Complete COMSEC documents may not be reproduced unless specific authorization is obtained from the originator of the publication. Instructions for reproducing extracts will be contained in the document's handling instructions.

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

107. Photography

a. No photographic equipment may be taken into areas where keying material is exposed or visible. All keying material must be secured in locked containers prior to photographic equipment being allowed into the area.

b. No photographs of the equipment interior may be taken. Official photographs of the equipment exterior may be taken. Official or unofficial photographs, drawings, or descriptive information for press releases or private use are prohibited.

c. Control of photographic equipment on board aircraft containing COMSEC material is the responsibility of the aircraft commander. Unofficial photography must be carefully monitored so as not to include photographs of COMSEC equipment either by limiting the area or panels photographed or by covering the equipment.

108. Public Display of COMSEC Material - COMSEC equipment and ancillary devices may be displayed at official functions such as symposia, open houses, etc., if authorities responsible for the handling and protection of the COMSEC equipment and ancillary devices ensure sufficient procedures exist to reasonably preclude theft, tampering, and other such unauthorized access. Equipment used for demonstration may be keyed with an unclassified sample or maintenance key only. The public display of operational keying material will not be permitted at any time.

ANNEX A

REFERENCES

The requirements of the referenced publications apply to this NSTISSI to the extent specified.

a. NSTISSD No. 502, National Security Telecommunications and Automated Information Systems Security, dated 5 February 1993

b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated 1997

c. AMSG-773, Policy and Procedures for Handling and Control of Two-Person Controlled (TPC) NATO Sealed Authentication System (SAS), dated January 1993

d. AMSG-293, NATO Cryptographic Instructions, dated January 1987

e. AMSG-505, NATO CRYPTO Distribution and Accounting Publication, dated December 1990

f. Chairman Joint Policy Governing Positive Control Material and Devices, CJCSI 3260.01, dated 31 July 1995

g. NSTISSI No. 4001, Controlled Cryptographic Items, dated July 1996

h. NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991

i. DCID 1/21, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities, dated 29 July 1994

j. NTISSI No. 7000, TEMPEST Countermeasures for Facilities, dated 29 November 1993

k. NTISSP No. 3, National Policy for Granting Access to U.S. Classified Cryptographic Information, dated 19 December 1988

l. NCSC-2, National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Non-governmental Sources, dated 7 July 1983

m. NSTISSP No. 8, National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments, dated 13 February 1997

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

o. NSTISSI No. 4006, Controlling Authorities for COMSEC Material, dated 2 December 1991

p. NSTISSI No. 4000, Communications Security Equipment Maintenance and Maintenance Training, dated 1 February 1991

ANNEX B

DEFINITIONS

With the exception of h and i. below, the following definitions are from NSTISSI 4009 (reference b. in ANNEX A of this NSTISSI). However, the information in brackets is pertinent to this NSTISSI only.

a. Access - Opportunity to make use of an information system resource. [An individual does not have access, if he or she is under escort or if a physical, technical, or procedural measure prevents them from obtaining knowledge or altering information, material, resources or components.]

b. COMSEC Facility - Space used for generating, storing, repairing, or using COMSEC material. [The material may be in either hard copy or electronic form. Unless otherwise noted, the term "COMSEC facility" as used in this NSTISSI refers to all types of COMSEC facilities, including telecommunications facilities, and includes platforms such as ships, aircraft, and vehicles.]

c. COMSEC Material - Item designed to secure or authenticate telecommunications. [COMSEC material includes, but is not limited to, key, equipment, devices, documents, firmware or software embodying or describing cryptographic logic, and other items performing COMSEC functions.]

d. COMSEC Material Control System (CMCS) - Logistics and accounting system through which COMSEC material marked CRYPTO is distributed, controlled, and safeguarded. [Included are the COMSEC central offices of record (COR), cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled through the CMCS.]

e. Electronically Generated Key - Key generated in a COMSEC device by introducing (either mechanically or electronically) a seed key into the device and then using the seed, together with a software algorithm stored in the device, to produce the desired key. [Electronically generated key may be encrypted or unencrypted; unless otherwise noted, the requirements of this NSTISSI apply to both encrypted and unencrypted electronic key. Electronically generated key stored magnetically is not considered hard copy key.]

f. Fixed COMSEC Facility - COMSEC facility that is located in an immobile structure or aboard a ship. [Heads of appropriate U.S. Government Executive Branch departments and agencies will determine what is categorized as a ship.]

g. Keying Material - Key, code, or authentication information in physical or magnetic form. [It includes key tapes and lists, codes, authenticators, one-time pads, floppy disks and magnetic tapes containing key, plugs, keyed microcircuits, electronically generated key, etc.]

h. Mobile COMSEC Facility - COMSEC facility that can be readily moved from one location to another. [This does not include ships that have been classified as fixed facilities.]

i. Telecommunications Facility - A type of facility dedicated to the preparation, transmission, communication or related processing of information. [Unless otherwise noted, the term "telecommunications facility" as used in this NSTISSI refers to both attended and unattended telecommunications facilities.]

ANNEX C

TRANSITION TO THE ELECTRONIC KEY MANAGEMENT SYSTEM

1. Key Management has had many changes over the years with various forms of key providing different benefits to the users. Currently, the management for all keying material is accomplished within the COMSEC material control system (CMCS), which requires the custodian to type in information about key received, transferred, or destroyed, as well as, to produce paper or floppy disk reports.

2. To improve the speed and efficiency of key management, the Electronic Key Management System (EKMS) has been developed to automate the CMCS and provide new capabilities for generating and managing electronic key. EKMS is not a separate key management system. The EKMS equipment can be used to track the CMCS material in all its forms. It also has an electronic link back to the Central Facility (CF) to place key orders, receive key material, and file accounting reports.

3. Providing a method to automate the account management and electronic methods for working with the CF will be a great benefit to COMSEC managers/custodians. The use of paper systems will be greatly reduced, and the time delay between ordering and receiving the keying material will be shorter. There will be a transition phase where keying material will be accounted for either manually or by EKMS equipment. A complete shift to an automated system will be accomplished in the near future.

4. The EKMS will show a clear distinction between the physical keys and the electronic keys to COMSEC account managers/custodians. Accounting Legend Code (ALC) 6 and ALC 7 were created for the specific purpose of designating electronic keys. ALCs 1, 2, and 4 remain the same and apply to physical material. This introduction of ALCs 6 and 7 provides the Account manager/custodian with a clear distinction between electronic and physical key.

5. When an account is required to perform an inventory, or process ALCs 1, 2, or 4 material, the ALC identifies the key as being in physical form. Electronic keying material will be identified by the ALC 6 or 7 which will indicate this material is being held within the EKMS equipment. Normally this indicates the key is stored in the Local Management Device/Key Processor (LMD/KP). Electronic key is different from physical key because the account manager/custodian cannot "touch" the key and must rely on the equipment for verification.

ANNEX D

HANDLING AND ACCOUNTING FOR ELECTRONIC KEY

1. Scope and Purpose - This ANNEX describes the doctrinal requirements for handling and accounting for electronic keys generated and distributed by elements of the Electronic Key Management System (EKMS).

2. Definitions - The following definitions pertain only to electronic key issues described in this ANNEX and are not included in reference b.

a. Electronic Key Management System (EKMS) - Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, accounting, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

b.

c.

d.

e.

f. Key Processor (KP) - Cryptographic component in EKMS designed to provide for the local generation of keying material, encryption and decryption of key, key load into fill devices, and message signature functions.

g. Local Management Device (LMD) - Component in EKMS which provides automated services for the management of key and other COMSEC material and an interface to the Key Processor. (It is composed of a user-supplied platform, an operating system, and EKMS software).

h. Local COMSEC Management Software (LCMS) - Software which resides on the LMD and performs EKMS functions such as accounting, auditing, distribution, ordering, production, system administration, operator interface services, and platform dependent services. (It provides the capabilities to manage and account for electronic key, physical key, and other COMSEC material such as equipment and manuals).

i. Data Transfer Device (DTD) - Fill device designed to securely store, transport, and electronically transfer keying material, designed to be backward compatible with the previous generation of COMSEC fill devices, and programmable to support modern mission systems.

3. Responsibilities of COMSEC Custodian - COMSEC custodians supporting LMD/KP will handle and account for the electronic keys as virtual rather than physical items. They are responsible for verifying the accuracy of all accounting reports involving electronic keys under their purview.

4. Definition of ALCs 6 and 7 - EKMS provides a clear distinction between the handling of hard copy key and electronic key to the COMSEC managers. ALCs 6 and 7 are specifically designed for electronic key management. (ALCs 1, 2, and 4 apply to hard copy key material).

a. ALC 6 key is centrally accountable to the central office of record (COR). When ALC 6 key is generated, including at Tier 1 or Tier 2, it must be reported to the COR. Electronic key produced by Tier 0 or Tier 1 will be assigned ALC 6.

b. ALC 7 key is locally accountable. Key generated locally by an LMD/KP will be assigned as ALC 7 or ALC 6.

5. Accounting and Reporting

a. Copies of physical key received and subsequently loaded into a key processor will be assigned an electronic short title and an ALC. ALC 1 will become ALC 6 and ALC 4 will become ALC 7. The electronic and physical versions will be both accounted for in LCMS. Physical key (e.g., KOI-18 Key Tape Reader) filled to a DTD will maintain its original short title. The DTD does not provide an audit trail.

b. Electronic keys converted to physical form in EKMS (e.g., key storage device) will be assigned a short title and an ALC code of 1 or 4, as directed by controlling authority (encryption, classification, etc. are factors in the assignment). The electronic key and the physical copies must be accounted for separately.

c. The local disposition records will be retained by the COMSEC manager/ custodian until the next audit after destruction of the keys or other COR-approved COMSEC inspection.

6. Issuing

a. Keys transferred electronically from the initial COMSEC account will be recorded as such by the LCMS. The LCMS should be used to print out a hand receipt which would provide a basis of receipt, inventory, and reconciliation for keys issued from the LMD/KP to a DTD. Alternate methods such as disposition statements are also acceptable.

b. The multiple copies of some keys issued from the DTD will be reflected in the audit trail; however, it is good practice to maintain hand receipts to allow identification of the recipient. Such procedures are needed to support compromise recovery. Copies of keys destroyed within 24 hours of being loaded into the data transfer device may be exempted from inventory. If the audit information is not examined, an individual must be present to witness the destruction.

c. Issuing on Floppy Disk

(1) If keys are issued by means of a floppy disk, the floppy disk will be classified SECRET and marked "SECRET, ALSO CONTAINS UNCLASSIFIED CRYPTO" (this is not equivalent to "SECRET CRYPTO"). An electronic Standard Form (SF)-153 is included in the individual, bulk-encrypted transactions on the medium, which may be composed of various short titles and editions. Keys on the floppy are assigned ALC 6, if they originally came from Tier 0 or Tier 1. These magnetic media may be transported to the subaccount or authorized user by any means approved for SECRET material. Once received, the media will be protected to the SECRET level under COMSEC control. Within three days of receipt, keys from these

EKMS floppies must be loaded into the LMD/KP and the media destroyed, degaussed, or overwritten as described in paragraph 6.c.(3), below.

(2) Floppy disks containing EKMS key may not be directly copied by the user (the contents of the floppies must be loaded into the LMD/KP, because it is not possible to determine the contents of the floppy without decrypting the bulk-encrypted transactions). The LMD key files may be backed up individually or in a more automated fashion. As a minimum requirement, the procedures for making backups should be documented in a facility security plan approved by the Facility Security Officer and COMSEC custodian, giving labeling information, storage location, classification, responsible personnel, etc. Ideally, local accountability per item should be maintained until the next audit, after the key is destroyed or a COR-approved COMSEC inspection, showing identification of the source material (short title, and, if possible, edition), number of copies made, to whom the material was issued, and disposition.

(3) Magnetic media containing encrypted electronic keys may be either destroyed or, if desired, degaussed or overwritten by an NSA-approved procedure for reuse. The floppy must be destroyed in accordance with regulations for destroying a floppy disk that contains classified SECRET data (disregarding the unclassified CRYPTO marking).

7. Storage - Keys stored in the memory of the computer hosting the LCMS must be stored in encrypted form. This computer will be classified SECRET and protected at that level. If a removable hard drive is used, then the hard drive, not the computer, will be classified SECRET.

8. Inventory - When the inventory of electronic key is performed by an EKMS component such as the LMD/KP, a witness is not required for this inventory. However, a witness is required for an inventory of keys in a DTD, if the audit information is not examined.

9. Destruction

a. Destruction of keys in the LMD/KP is accomplished by zeroization of the KP and the initialization keys or deletion of keys from the account; if the destruction report is forwarded electronically, a witness is not required. An individual is not required to witness the destruction or inventory of electronic key where the destruction or inventory is performed by an EKMS component such as the LMD/KP. When destroying keys issued electronically to a subaccount or authorized LMD, the COMSEC custodian must maintain records certifying the witnessed destruction was performed, if the report was provided in hard copy.

b. Destruction of keys issued to a DTD is accomplished by deletion. This must be verified by the COMSEC custodian or two authorized users by viewing the display of the DTD contents or its audit trail. Destruction must be reported back to the issuing LMD/KP. The LMD/KP must then report the disposition to the COR.

10. Audit - Inventories will be provided by the COR to assist in audits.

ANNEX E

DETERMINING HIGH RISK OF CAPTURE ENVIRONMENT

The following table provides a guide for determining whether a particular environment poses a high risk of capture by an adversary. Responsible officials should select one situation from each category and add the points. Any scenario totaling 15 points or higher is considered high risk; however, the guide is not all inclusive. Responsible officials may declare a high risk environment whenever circumstances warrant. In a training environment, the risk assessment should be based on the training scenario rather than actual environment.

Category 1 - Location	
U.S. and its possessions	0
Allied countries and international waters	1
Non-allied countries	5
Countries hostile to the U.S.	10
Disputed territories and demilitarized zones	15
Category 2 - Operational Environment	
Static environment	0
Mobile or tactical situation in the U.S.	5
Mobile or tactical situation outside of the U.S.	10
Battlefield (air, land, or sea)	15
Category 3 - Government Stability	
Law and order being maintained	0
Terrorist or effective dissident activity; rioting:	
Police or military activity	7
Coup d'etat imminent; anarchy	15
Category 4 - Supporting Guard Forces	
Significant U.S. or allied armed forces in local area	0
Limited U.S. or allied armed forces in local area	2
Small U.S. or allied guard force at activity, but no other U.S. or allied armed forces in local area	5
No supporting guard forces	7

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

CNSS-045-05
28 September 2005

National Manager

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

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Amendment to NSTISSI No. 4005 – **ACTION MEMORANDUM**

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

2. (U) Please add the enclosed ANNEX F to your original copy of this document.

/s/
KEITH B. ALEXANDER
Lieutenant General, U.S. Army

Encl.
a/s

(U) NSTISSI No. 4005, ANNEX F, dated 9/28/2005

(U) SAFEGUARDING COMSEC MATERIAL IN ELECTRONIC FORM

(U) SECTION I – PURPOSE

1. (U) This ANNEX provides guidance for situations not covered adequately by the basic instruction. Guidance in this ANNEX relaxes policy for material encrypted by NSA approved cryptography. The premise of this ANNEX is that COMSEC Material encrypted via NSA approved means is subject to less restrictive safeguarding and control requirements than unencrypted COMSEC Material.

a. In those instances where this ANNEX is in conflict with the basic instruction, this ANNEX will govern.

b. Service/Agency policy/procedures, and local policy/procedures may make the procedures contained herein more stringent but may not relax the requirements herein.

c. Systems or equipment security doctrine promulgated by NSA may contain specific procedures that override both the basic instruction and this ANNEX for that specific system or equipment only.

(U) SECTION II - DEFINITIONS

2. (U) Definitions and acronyms contained in the National Information Assurance (IA) Glossary, CNSSI No. 4009, apply to this ANNEX. Additional or modified definitions that are applicable to this ANNEX follow:

a. (U) COMSEC Material – Item(s) designed to secure or authenticate information. COMSEC material includes, but is not limited to: key, products, equipment, modules, devices, documents, hardware, firmware, or software that embodies or describes cryptographic logic, and other items that perform COMSEC functions.

b. (U) COMSEC Software – Includes all types of COMSEC material, except key, in electronic or hard copy form. This includes all classifications of unencrypted software, and all associated data used to design, create, program or run that software. It also includes all types of source/executable/object code and associated files that implement, execute, embody, contain, or describe cryptographic mechanisms, functions, capabilities, or requirements. COMSEC software also includes Transmission Security (TRANSEC) software and may include any software used for purposes of providing confidentiality, integrity, authentication, authorization, or availability services to information in electronic form.

c. (U) CRYPTO – The marking or designator identifying unencrypted COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information. This includes non-split keying material used to encrypt/decrypt COMSEC critical software and software based algorithms.

d. (U) Encrypted Key – Key that has been encrypted in a system approved by NSA for key encryption. This ANNEX assumes the key's unencrypted associated data (e.g., header or tagging information) is not sensitive. See paragraph 3 below.

e. (U) Encryption – Whenever used in this document, the words "encrypt" or "encryption" refer to an NSA process approved for protection of the given keying material.

f. (U) Personal Identification Numbers (PINs) – A series of letters, special characters, and numbers known only to authorized persons, used to enable access to the secure functionality of COMSEC products/equipment.

(U) SECTION III – CLASSIFICATION AND MARKING OF ENCRYPTION KEYS AND ENCRYPTED COMSEC MATERIAL

3. (U) Data Associated With Encrypted Key. Encrypted key may have classified or sensitive data (e.g., header or tagging information) associated with it. The associated data may or may not be encrypted. If the associated data is not encrypted, the entire data package may be sensitive or classified.[1] When possible, the sensitivity of the associated data will be specified in equipment systems security doctrine or applicable classification guidance. NSA in conjunction with the Controlling Authority and user community will make this determination. Note: Encrypted data is not considered CRYPTO.

4. (U) Encrypted key, which is not derived from benign keying techniques, must be safeguarded and controlled separately from its associated unencrypted Key Encryption Key (KEK) until loaded into the end cryptographic unit (ECU) or approved fill device. If this is not possible, the encrypted key must be classified to the level of the underlying information. If kept separate from its associated KEK, encrypted keying material is UNCLASSIFIED//FOUO. Systems security doctrine provides procedures for specific equipment containing both encrypted key and its associated KEK. Absent such doctrine, equipment containing both encrypted key and its associated KEK are considered to hold unencrypted key.

5. (U) Encrypted COMSEC software and all associated encrypted software outside an ECU must be safeguarded and controlled separately from the key splits/keys, which when combined together provide the ability to decrypt the software. If this is not possible, both the key and software must be considered classified to the level of the information being protected. Electronic key is considered to be stored separately if, without proper authorization, the key can

[1] (U) e.g. if the membership list of a net is sensitive, then sending each member the same encrypted key with an unencrypted header specifying the key's short-title may be a sensitive operation and should be protected.

not be accessed, viewed, copied, transferred, etc., and the encrypted software cannot be joined with its associated keys.

6. (U) Encrypted algorithms shall not be marked CRYPTO. They may be safeguarded and controlled outside the COMSEC Material Control System (CMCS). Note: Unencrypted classified algorithms are controlled in the CMCS and handled as specified in paragraphs 54.c, 60.c, 88 and 106.c. of the basic instruction. (See also 13.b. below.)

7. (U) Keying material and COMSEC software encrypted via an NSA approved means, are considered UNCLASSIFIED//FOUO unless the systems security doctrine directs otherwise. Use of specific media/systems may necessitate additional safeguarding and control requirements.

8. (U) Unencrypted key used to encrypt COMSEC material must be safeguarded and controlled in accordance with the classification of the information being protected, unless the systems security doctrine directs otherwise.

9. (U) Split Key. If a key used to encrypt or decrypt classified software is split, at least one of the key splits must be safeguarded and controlled in accordance with the classification of the information being protected. Classified key splits are accountable keying material for control and access purposes. (See paragraph 14.) Specific systems security doctrine defines keying material control requirements for each equipment and may differ from this general requirement.

10. (U//~~FOUO~~)

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

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

11. (U) Encrypted key, encrypted software and other encrypted data may be sent via means authorized for UNCLASSIFIED//FOR OFFICIAL USE ONLY data, e.g., SIPRNET or NIPRNET. NIPRNET use requires the use of approved protection measures, e.g., medium assurance PKI encryption. Tracking, control, or accounting, if required, shall occur as if the data were sent in physical form. (See also paragraph 18.b below.)

(U) SECTION IV – SAFEGUARDING, CONTROL, AND DESTRUCTION

12. (U) Safeguarding and Control of Encrypted Key and Software. Encrypted key and encrypted software without special control and safeguarding requirements should be treated as UNCLASSIFIED//FOR OFFICIAL USE ONLY material. The system, Service, or user may require tracking, control, or accounting for encrypted software and encrypted key, depending on the application.

13. (U) Control and safeguarding.

a. (U) Encrypted COMSEC Software is not accountable in the CMCS, nor is it a Controlled Cryptographic Item (CCI). It may be safeguarded and controlled as UNCLASSIFIED//FOUO data that requires no audit or accounting (unless required by systems security doctrine or local policy) as long as it remains separate from its decryption keying material.

b. (U) Unencrypted operational classified COMSEC software in electronic form will be accounted for in the CMCS with the following exceptions:

(1) (U) CMCS accounting is not required for unencrypted classified COMSEC software in development (pre-production) environments (e.g., in a controlled area at a government or contractor facility); however, normal safeguarding, accounting, configuration control, and access rules for classified COMSEC material continue to apply.

(2) (U) CMCS accounting is not required for software inside an ECU (i.e., once loaded into an equipment from which it cannot be extracted).

c. (U) Unencrypted non-COMSEC Software (e.g., mission data, radio parameters) may be safeguarded and controlled as non-CMCS-accountable data. If the software is classified, it must be safeguarded and controlled at the appropriate classification level.

d. (U) Encrypted keying material is not CRYPTO. Once a data package containing encrypted keying material is received and decrypted, no further accounting for the original encrypted data package is necessary. The decrypted keys will then be safeguarded, controlled, and accounted for per existing procedures for unencrypted key.

e. (U) Unencrypted keying material intended to encrypt operational data will remain CRYPTO and will be accounted for in the CMCS.

NOTE: (U) Keys that are decrypted and exposed to human view/intervention must be accounted for in the CMCS. Keys decrypted in a machine system from which unencrypted key cannot be extracted (e.g., benign fill equipment) do not need additional accounting.

14. (U) Accounting Legend Code (ALC). Key and key splits in electronic form used to protect software algorithms or software that performs cryptographic functions will be assigned ALC 7 (preferably) or ALC 6, based on system requirements. Such key or key splits, when in physical form (e.g., on a KSD-64 or a floppy disk), must be safeguarded and controlled in the CMCS as ALC 1 or ALC 4 items, depending on specific program requirements as documented in specific systems doctrine. Regardless of the ALC assigned, such key or key splits are not marked CRYPTO. The EKMS Tier 0 may generate such ALC 6 or 7 material.

15. (U) Controlling Authorities must be able to identify and verify the secure communications requirement for their cryptonet for all users of their key. Thus, key may only be sent to a user with the Controlling Authority's permission. This includes key used to protect COMSEC software.

16. (U) It may be required by systems security doctrine, local authorities, or as an intrinsic part of the specific system itself, that the user, system or Service/Agency 1) track the movement and use of software encryption key splits and encrypted software packages and 2) maintain configuration and version control of the software. This may be done locally or at a central database. At a minimum, local users who load the software encryption key/splits should ensure written records are maintained, listing the date, time and the version of software loaded for all terminals under their control.

17. (U) Key may be generated at EKMS Tier 0 at the UNCLASSIFIED level.

18. (U) Distributing Key on Floppy Disk, CD ROM or Other Removable Storage Media.

a. (U) If key is distributed from an EKMS account other than Tier 0 by means of a removable storage media, the media must be classified SECRET since these systems are SECRET system high.

(1) (U) Media extracted from a SECRET-high system must retain the classification of the system.

(2) (U) SECRET media (e.g., from an LMD or Tier 1) containing encrypted key may be declassified using procedures approved by appropriate local authorities.

(3) (U) The notice "COMSEC ACCOUNTABLE" and a short title shall also be physically present on the media to indicate that the media must be tracked within the CMCS.

(4) (U) The LMD may only distribute encrypted key. An electronic SF-153 is included in EKMS bulk encrypted transactions (BETs) on the medium.

b. (U) SECRET magnetic media containing encrypted keying material may be transported to the subaccount or authorized user by any means approved for SECRET collateral material. (See also paragraph 11 above.) Once received, the media must be safeguarded and controlled at the SECRET level.

c. (U) As soon as practical after receipt, EKMS media containing bulk-encrypted transactions must be loaded into the designated LMD/KP in order to verify the integrity of the data. The EKMS media or any non-EKMS media containing encrypted keying material may then be degaussed or overwritten (if appropriate to the media) following approved procedures, and then reused in accordance with established local procedures, or the media may be destroyed following approved procedures. Data from the bulk-encrypted transactions will subsequently be part of the LMD/KP database backup.

d. (U) EKMS media should not be copied as the data on the media is encrypted for one specific LMD/KP and cannot be used elsewhere. The contents of the floppies must be loaded into the LMD/KP as soon as practical, because it is not possible to determine the contents of the floppy without decrypting the bulk-encrypted transactions.

19. (U) Destruction.

a. (U) Encrypted key should be destroyed when no longer needed or upon supersession of the keying material.

b. (U) Electronic keying material, except for KEKs, filled into an ECU may be securely stored in an approved key fill device until the supersession date of the key, when operationally necessary. KEKs must be destroyed as soon as they are filled into the ECU unless specific systems doctrine allows further retention. The key fill device must create and store an audit trail capable of indicating when and how many times each key was output from the fill device.

(U) NOTE: This allowance excludes the KYK-13 and KYX-15, which have no audit trail capability. (Users of the KYK-13 and KYX-15 must continue to follow paragraph 77.c. of the basic instruction.) It does include the Data Transfer Device (DTD), the Secure DTD2000 System (SDS), and Simple Key Loader (SKL).

(U) To ensure only authorized copies of keying material are made, the audit trail from the fill device must either be uploaded to an LMD/KP where it will be reviewed, or viewed on the fill device itself by the local COMSEC Custodian or COMSEC Officer. Audit trail review times will be specified in systems doctrine.

c. (U) The destruction technique for electronic key depends on its state (encrypted vs. unencrypted) and the media/equipment on which it resides. Routine Destruction and Emergency Protection of COMSEC Material, NTISSI No. 4004 (reference h), section 4.a, dated 11 March 1987, states that "Keying material designated CRYPTO that has been issued for use should be destroyed as soon as possible after supersession, and may not be held longer than 12 hours following supersession." This requirement remains for hardcopy keying material, but for electronic key it is superseded by the following guidance:

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

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

(2) (U//~~FOUO~~)

NOTE: All unencrypted copies of electronic keys must be destroyed within 12 hours following supersession, or in accordance with paragraph 19.c(1) above, or in accordance with NSTISSI No. 4005 paragraph 40 (where encryption constitutes protective packaging), whichever is applicable. Destruction of copies of unencrypted key on magnetic storage media must be done in accordance with NSTISSI No. 4005 paragraph 77.g.

20. (U) Classification of Passwords and Personal Identification Numbers (PINs). (Note: Passwords and PINs are referred to collectively as PINs hereafter.) PINs will normally be assigned the highest classification of any information protected by the PIN. If the PIN used to unlock the secure capability of a device cannot be associated with that particular device within the amount of time the device is expected to be unattended, and the PIN is properly safeguarded and controlled per local policy, the PIN may be considered UNCLASSIFIED//FOR OFFICIAL USE ONLY.

(U) SECTION V – REPRODUCTION

21. (U) Reproduction. COMSEC material is reproduced when it is duplicated in like form (e.g., creating a backup copy of a disk) or converted for equipment fill (e.g., extracting a key file from a disk and storing it on a computer or key transfer device). Converting hard copy key to electronic form for immediate equipment fill is not considered reproduction. Reproduced material must be documented and controlled in the same manner as the original material in accordance with department or agency directives.

a. (U) Keying material for machine cryptosystems will not be reproduced without the consent of the controlling authority. If controlling authority approval cannot be obtained in time to meet operational requirements, or if a controlling authority cannot be identified, the local commander can authorize reproduction. The Central Office of Record (for ALC 6 key only) and the controlling authority must be notified at the earliest opportunity.

b. (U) Unencrypted cryptographic algorithms and COMSEC software will not be reproduced without the authorization of the NSA Information Assurance Policy, Procedures, and Insecurities Division (I01P).

c. (U) Encrypted cryptographic algorithms and COMSEC software may be reproduced as necessary. Sensitive programs, e.g., Nuclear Command and Control programs, may require additional controls. Such controls will be found in specific systems security doctrine, which have precedence over this ANNEX.

(U) SECTION VI – SUMMARY

22. (U) The following table summarizes the guidance given in this ANNEX.

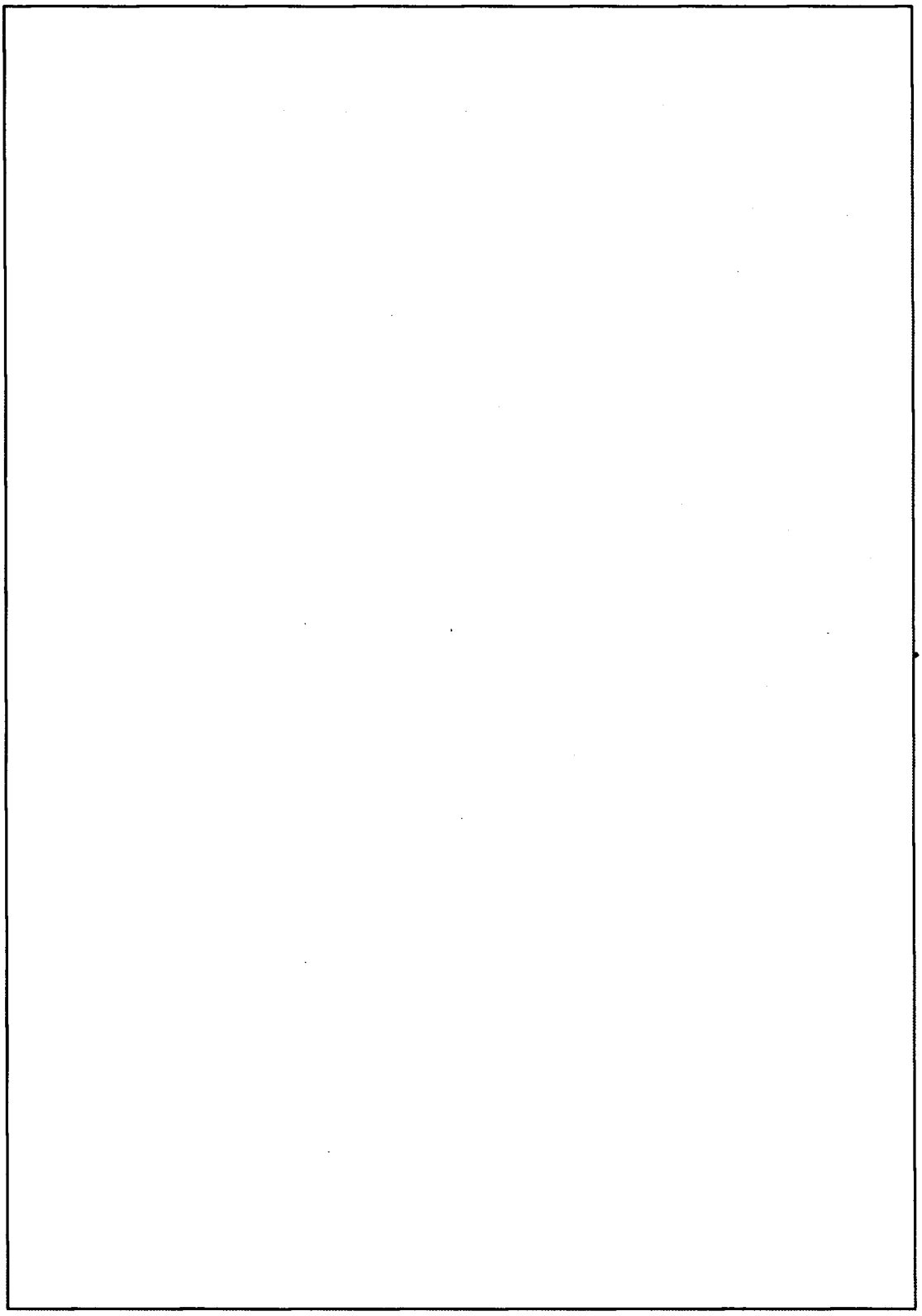
	Classification// Marking	CMCS Accounting[1]	CRYPTO Marking
Key – Unencrypted	Level of material	Yes	Yes
Key – Encrypted	UNCLASSIFIED// FOUO[2]	No	No
Software* – Unencrypted	Level of material	Yes	No
Software* – Encrypted	UNCLASSIFIED// FOUO	No	No
(Split) Key which encrypts/decrypts COMSEC Software	Level of material	Yes	No
Encrypted Data	UNCLASSIFIED	No	No

*Software includes cryptographic algorithms.

[1] (U) Note: CMCS Accounting requires the assignment of a nomenclature to the item by NSA.
[2] (U) Unless sensitive associated (unencrypted) data raises the classification. See paragraph 3.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:



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