



DEPARTMENT OF THE NAVY
U.S. NAVAL COMPUTER AND TELECOMMUNICATIONS STATION
PSC 488 BOX 101
FPO AP 96537-1800

NCTSGUAMINST 2280.1U
N00SM
26 Jun 15

NAVCOMTELSTA GUAM INSTRUCTION 2280.1U

From: Commanding Officer, U.S. Naval Computer
Telecommunications Station, Guam

Subj: STANDARD OPERATING PROCEDURES (SOP) FOR HANDLING,
ACCOUNTABILITY, TRANSMISSION, AND DISPOSITION OF
COMMUNICATION SECURITY (COMSEC) MATERIAL

Ref: (a) EKMS 1 (Series)
(b) EKMS 3 (Series)
(c) EKMS 5 (Series)
(d) NAG 16 (Series)
(e) SECNAVINST M5510.36 (Series)
(f) SECNAVINST 5510.30 (Series)
(g) EKMS for Commanding Officer's Handbook

Encl: (1) Table of Contents
(2) Sample Letter of Appointment
(3) SD Form 572
(4) STE Statement of Responsibility Form
(5) COMSEC Material Required Reading List
(6) EKMS Local Element Training
(7) Audit Teams Command Periodic Review Guide
Check List
(8) Watch-to-Watch Inventory Form
(9) Electronic Key Transfer/Over-the-Air-Transfer
EKT/OTAT Key Generation Log
(10) Data Transfer Device User Guide
(11) Data Transfer Device/Simple Key Loader Audit Log
(12) Destruction Procedures
(13) Over-the-Air-Rekey/Over-the-Air-Transfer (OTAR/OTAT)
Policy
(14) Watch to Watch Inventory Procedures

1. Purpose. To promulgate instruction for safeguarding COMSEC Material at NCTS Guam and the commands and elements it supports, through the Electronic Key Management System (EKMS).

2. Cancellation. NCTSGUAMINST 2280.1T

3. Background. In addition to references (a) through (g), this instruction provides local Management guidance for the accounting, distribution, destruction, and management of electronic keys, as well as management of physical key and non-key COMSEC related

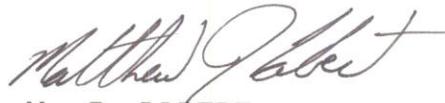
items. Key management continues to evolve and these technologies are governed by both National and Navy policy. The goal of this

policy is to balance timely COMSEC support to a global user community while enhancing security and minimizing costs.

a. NCTS Guam is the Parent account (TIER 2) for shore based Navy commands and various other DOD entities located on Guam. The NCTS Guam EKMS account number is 259015 and the account is further extended to subordinate internal and external Local Element (LE) accounts.

4. Scope. The policies in this instruction have been derived from those set forth in NSA, OPNAV, SECNAV and other National and Navy-level COMSEC policy manuals. This guidance supplements but in no way alters or amends the provisions of SECNAV M5510.30 (series), SECNAV M5510.36 (series) or U.S. Navy regulations.

5. Action. All personnel performing EKMS duties shall be familiar with the contents of this directive. If at any time, the Local Element Custodian/Alternate or Users of COMSEC material are unsure of how to handle a particular requirement or situation, contact the EKMS Office at 355-5887 or NCTS Guam Command Duty Officer at 688-3497.



M. J. LABERT

Copy to:
NCTS, Guam EKMS Manager
NCTS, Guam
All Local Elements

TABLE OF CONTENTS

<u>TOPIC</u>	<u>PAGE</u>
Introduction to Communications Security	3
Introduction to the Electronic Key Management System (EKMS)	3
Operating Principles of EKMS	4
Records and Files	4
Handling and Storage of EKMS Material	6
Access Restrictions and Controls	10
Responsibilities and Duties: Commanding Officer, NCTS GUAM	11
Responsibilities and Duties: EKMS Manager and Alternate(s)	12
Responsibilities and Duties: Local Element (LE) Commanding Officer	14
Local Element Custodian (LEC)	17
Return / Transfer of Equipment	19
Responsibilities and Duties: EKMS Users	20
Safeguarding COMSEC Material and Facilities	20
Inventories	20
Amendments	21
Over-The-Air Transfer/Over-The-Air-Rekey (OTAT/OTAR)	21
Disposition and Destruction of COMSEC Material	21
COMSEC Incidents and Practices Dangerous to Security (PDS)	25
Data Transfer Device (DTD) and Simple Key Loaded (SKL)	25
Introduction to the Secure Terminal Equipment (STE)	25
Emergency Action Plan (EAP)	26
Notification	27

1. Introduction to Communications Security.

a. Communications Security (COMSEC) is used to protect U.S. Government and partner transmissions, communications, and the processing of classified or sensitive unclassified information related to national security from unauthorized persons/access; COMSEC Material is used to ensure the authenticity and integrity of such communications.

b. The protection of vital and sensitive information moving through government communications systems is crucial to the effective conduct of the government and specifically to the planning and execution of military operations.

2. Introduction to the Electronic Key Management System (EKMS).

a. EKMS is an interoperable collection of systems, facilities, and components developed by the services and agencies of the U.S. Government to automate the planning, ordering, filling, generation, distribution, accountability, storage, usage, destruction and management of electronic key and other types of COMSEC material. The Local Element is considered part of the TIER 3 layer of the EKMS architecture and can include the AN/CYZ-10 (Data Transfer Device (DTD), AN/PYQ-10 (Simple Key Loader (SKL) or other means used to fill key to End Cryptographic Units (ECUs).

b. EKMS is unique in that each item of material, whether keying material (KEYMAT) or COMSEC equipment (Controlled Cryptographic Item (CCI), is identified by a distinctly different short title, edition, and in most cases an accounting number. Every piece of COMSEC material that is charged to your account is assigned an Accountability Legend (AL) Code. The AL Code determines how COMSEC material is accounted for within the EKMS. Five AL codes are used to identify the minimum accounting controls required for COMSEC material. The degree of accountability required for each AL code follows:

Physical Keying material and CCI Equipment

c. AL Code 1: COMSEC material is continuously accountable to the Central Office of Record (COR) by accounting (serial/register) number from production to destruction.

d. AL Code 2: COMSEC material is continuously accountable to the COR by quantity from production to destruction.

e. AL Code 4: After initial receipt to the COR, COMSEC material is locally accountable by quantity and handled/safeguarded based on its classification.

Electronic Keying Material

f. AL Code 6: COMSEC material that is electronically generated and continuously accountable to the COR from production to destruction.

g. AL Code 7: COMSEC material that is electronically generated and locally accountable to the generating facility.

3. Operating Principles of EKMS. The operating principles of EKMS are based on the following safeguards:

a. A continuous chain of custody receipts by use of transfer reports and local custody documents.

b. Positive accounting records, such as periodic inventory reports, destruction records, transfer reports, and local custody records.

c. The requirement for immediate reporting of COMSEC Incident and Practice Dangerous to Security (PDS).

4. Records and Files.

a. Per reference (a) Chapter 7, the following records and files will be maintained by the EKMS Manager, NCTS Guam and the LE's (all records and files must be retained in accordance with reference (a), Annex S:

(1) Chronological File

(2) Correspondence, Messages and Directive File

(3) General Message File

(4) Local Custody File

b. A current COMSEC Library must be maintained by NCTS Guam and made available to all LE's. In accordance with reference (a), Article 721, the following items are minimum requirements for the COMSEC Library:

- (1) EKMS 704 - LMD/KP Operator's Manual
- (2) EKMS Intelligent Computer Aided Trainer (ICAT)
- (3) EKMS Manager Job Qualification Requirement (JQR)
- (4) COMPACFLT C2282.1(Series) - Shipboard Allowance of
COMSEC
- (5) EKMS 1 (Series) - EKMS Policy and Procedures for Navy
EKMS
- (6) EKMS 3 (Series) - EKMS Inspection Manual
- (7) EKMS 5 (Series) - EKMS Cryptographic Equipment Manual
- (8) NAG 53 (Series) - Keying Standard for Non-Tactical
KG-84/KIV-7 Point to Point Circuits
- (9) NAG 16 (Series) - Field Generation Over-the-Air-
Distribution (OTAD) of COMSEC Key
- (10) NSA Mandatory Modification Verification Guide (MMVG)
- (11) OPNAVINST 2221.5 (Series)
- (12) SECNAVINST M5510.36 (Series)
- (13) SECNAVINST M5510.30 (Series)
- (14) OPNAVINST 5530.14 (Series)
- (15) SECNAVINST 5040.3 (Series)
- (15) NAVICPINST 2300.4 (Series)
- (16) NAVICPINST 5511.24 (Series)
- (17) OPNAVINST 2221.3 (Series)
- (18) SDIP 293
- (19) AMSG 600

c. A Transaction Status Log must be maintained in accordance with, Article 724 of reference (a), by NCTS Guam.

The Transaction logs will be closed out at the end of each calendar year and retained in accordance with reference (a), Annex T.

d. The EKMS Manager and Local Element Custodians shall maintain a log tracking all COMSEC Material leaving the authorized storage spaces for daily use. The log shall contain the following items:

- (1) Date out
- (2) User name (print and signed)
- (3) Destination of COMSEC Material
- (4) Items (list by short title)
- (5) Date of return

5. Handling and Storage of EKMS Material.

a. At all times, all COMSEC material must be protected and safeguarded against loss, compromise, and unauthorized disclosure. All personnel requiring access to COMSEC material are to be designated in writing by means of an access roster maintained by the LE Manager and signed by the LE Commanding Officer.

b. All military personnel except those assigned to MSC, USCG, and USMC accounts appointed or designated as EKMS Managers, Alternates, LEs Issuing and LE Users, appointed/designated, must complete the applicable portions of the latest version of NAVEDTRA 43462 (EKMS PQS) for the position they are fulfilling (there is no PQS for a witness). The PQS is available from <https://www.netc.navy.mil/development.aspx>. In accordance with reference (a), Article 312

c. LE's will routinely receive physical and/or electronic COMSEC material from the NCTS EKMS Manager. They will be required to receive this material utilizing the established issue of material procedures in accordance with reference (a), Article 736. The SF-153 is used to document the receipt of all COMSEC material (including keymat, crypto equipment and Controlled Cryptographic Item (CCI) and requires two authorized LE signatures.

d. Two-Person Integrity (TPI)

(1) Definition. TPI is the system of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

e. Material requiring TPI at the Parent account and Local Element level.

(1) TPI (continuous presence of two authorized/cleared personnel and the material or container when opened) must be applied to the following COMSEC material from time of receipt through turn-in to the EKMS Manager or Alternate, or destruction:

(a) All TOP SECRET paper keying material marked or designated CRYPTO.

(b) Whenever unencrypted electronic keying material classified TOP SECRET is issued, generated, transferred (OTAR/OTAT), relayed or received. TPI is not required for distant ends responsible for circuits supported via OTAR except when the required KEK is loaded; OTAR does not involve extraction of key on the distant end.

(c) Fill Devices (FDs) containing unencrypted TOP SECRET key.

(d) Unloaded FDs in an operational communications environment containing keyed crypto-equipment from which TOP SECRET key may be extracted.

(e) Equipment that generates (KG-83/KGX-93) and allows for the extraction of unencrypted TOP SECRET key such as KG-83s. Specially designed locking bars are available for these devices and may be used to satisfy TPI requirements.

(2) Exceptions to TPI Requirements for COMSEC Keymat

(a) Mobile users or Navy Expeditionary Combatant Commands (NECC) (i.e., USMC tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion units,

Explosive Ordnance Disposal (EOD) units, and Mobile Inshore Undersea Warfare units (MIUWUs) are exempt from TPI requirements only while operating in a tactical exercise or operational field environment.

(b) Aircraft: TPI is not required for (Field Devices (FD)s during the actual loading process in the aircraft, but TPI is required on loaded FDs which contain unencrypted TOP SECRET key up to the flight line boundary.

1. Loaded FDs placed in an Air Crew Comm Box locked with TPI approved combination locks fulfills TPI requirements. Consequently, one air crewmember may transport the locked Comm Box up to the flight line boundary.

2. Loaded FDs may be stored onboard the Aircraft in a single-lock container while the aircraft is in flight status.

(c) Users in a totally SECRET or below environment are not required to maintain TPI for FDs.

(d) And others occasions list in reference (a) Article 510.

(e) Any loss of TPI required by this manual must be reported in accordance with reference (a) Article 945 as a physical incident.

f. Store COMSEC material separately from other classified material (e.g., in separate containers or in separate drawers) and segregate material by status (effective, ROB, superseded), type (keying material, paper COMSEC material, Aids) and classification (Top Secret (TS), Secret, Confidential, Unclassified). At the LE level, segregation will be by classification and type as LEs generally do not have Reserve on Board (ROB) material and any superseded material would be pending destruction which must occur within 12 hours of supersession or next opening of the container for a non-watch environment. This will ensure, if directed that material destroyed during emergency destruction is destroyed based on the sensitivity of the material and potential impact a possible compromise would have. The Emergency Action Plan (see para 9.I) must also be considered when organizing this material.

26 Jun 15

(1) COMSEC keying material designated for North Atlantic Treaty Organization (NATO) use may be stored with other COMSEC material.

g. Strict accountability and control of all EKMS material assigned to the watch or duty section must be maintained. In a continuously manned facility, a security check will be conducted once per shift, at least once every 24 hours, to ensure all classified COMSEC information is properly safeguarded, and physical security protection systems/devices (e.g., door lock and vent covers) are functioning properly.

h. In a non-continuously manned facility, conduct a security check prior to departure of the last person to ensure the facility entrance door is locked and, where installed, Intrusion Detection Systems (IDS) are activated. Document the check on an End of Day Security Checklist (SF-701).

i. If a facility will be unmanned for periods greater than 24 hours (e.g., during weekends and holidays), the facility will be protected by an approved IDS. A security check must be conducted and documented on the Security Container Check Sheet SF-702 at least once every 24 hours to ensure that all doors to the facility are locked, and that there have been no attempts at forceful entry. SF-701s and SF-702s will be retained in accordance with Annex T.

j. Under no circumstances will EKMS material be issued to non-EKMS cleared personnel. Immediately upon receipt of the EKMS material, LE's are directed to proceed without delay to the authorized facility where the material will be used or stored. If delays are anticipated from receipt to storage, material shall be held at the point of origin until it can be transported safely and without delay.

k. Store COMSEC material only in containers and spaces approved for their storage. Unless COMSEC material is under the direct control of authorized persons, containers and spaces shall be closed and locked.

(1) Storage Container Requirements. Storage containers for COMSEC keying material must have two locks, or if an electromechanical lock is used, it must be programmed in the dual combination mode for access. All locks will remain locked when not under the direct supervision of two appropriately cleared and authorized personnel.

(2) Storage containers for COMSEC material require the following MANDATORY forms:

- (a) SF-700 (Security container information)
- (b) SF-702 (Security container Open/closure log)
- (c) Optional Form-89 (Maintenance record)

(d) Open safe instructions will be clearly posted inside vault doors and security containers. The instructions should clearly identify who to call and what to do if a vault door or security container is found open. The following example is provided:

**OPEN SAFE INSTRUCTIONS
IF THIS CONTAINER IS FOUND OPENED AND UNATTENDED
IMMEDIATELY CARRY OUT THE INSTRUCTIONS LISTED BELOW:**

**DO NOT ENTER OR EXAMINE CONTENTS - NOTIFY THE
CDO AT (XXX - XXXX)**

**POST TWO GUARDS UNTIL PROPERLY RELIEVED BY PROPER AUTHORITY
PERSONNEL LISTED ON THE SF-700 FORM WILL BE NOTIFIED
AND REQUIRED TO CONDUCT AN INVENTORY OF THE CONTENTS
NOTIFY THE EKMS MANAGER OR ALTERNATE MANAGER(S)
IMMEDIATELY (XXX - XXXX)**

6. Access Restrictions and Controls.

a. Limit unescorted access to individuals whose duties require such access, and who meet the access requirements of reference (a), Article 510.

b. The names of persons having regular duty assignments in COMSEC spaces will be indicated on a command access list. The access list must be continuously vetted and updated to keep accurate without flaw or error. The access list must be promulgated to the EKMS vault immediately upon signature.

c. The responsible authority, Command Security Managers, may grant access to cleared and un-cleared visitors, provided they require such access. A properly cleared person whose name is on the access list must continuously escort un-cleared visitors.

d. When un-cleared persons such as repairmen are admitted to perform maintenance on commercially contracted information processing equipment connected to circuits protected by cryptographic equipment, the escort shall be a CRYPTO repair person or other technically qualified person capable of detecting malicious operations by the repairmen.

e. Record all visitors (personnel not on the access list) on a visitor log and retain the log for at least 1 year. The visitor register, at a minimum, will contain the following:

- (1) Date/time of arrival and departure
- (2) Printed name and signature of visitor
- (3) Command/Unit/Organization of visitor
- (4) Purpose of visit
- (5) Signature of authorized individual admitting the visitor(s)

f. Storage of Safe Combinations. EKMS safe combinations will be stored in accordance with, reference (a), Article 520. In addition, combinations of TPI EKMS safes will not be stored in the same security safe the combination accesses. EKMS safe combinations may be co-located with non-EKMS combinations provided they are physically segregated and appropriately marked.

7. Responsibilities and Duties: Commanding Officer, NCTS GUAM.

a. The CO, NCTS GUAM is ultimately responsible for the safe custody, proper handling, transmission, procedures, and disposition of EKMS distributed under his or her jurisdiction in accordance with reference (a), Article 450.

8. Responsibilities and Duties: EKMS Manager and Alternate(s).

a. The EKMS Manager and Alternate(s) are equally responsible for the administration and proper handling of EKMS material and equipment contained within the authorized allowance of the EKMS account.

b. The EKMS Manager and Alternate(s) are equally responsible for issuing EKMS material to local Users and administering guidelines, procedures, and training related to COMSEC for handling and care of material.

c. Additional EKMS Manager requirements may be found in reference (a), Article 440.d.

d. All EKMS Inventories shall be conducted in accordance with reference (a), Article 766.

(1) The EKMS Manager shall generate a local inventory for each vault or assign each vault as a local element within Local COMSEC Management Software (LCMS). A separate inventory of separate local elements will allow the vaults to be quickly inventoried if a compromise must be ruled out.

(a) Inventories shall contain the following items: short title, edition, date removed, date entered, personnel involved, destination of material.

(b) The local inventory sheet shall be updated as necessary, or whenever an inventory IAW reference (a) is executed.

(2) Completed inventories from LE's and their detachments shall be retained by the EKMS Manager for the same duration as NCTS Guam inventories.

e. EKMS KEYMAT and COMSEC destruction must be conducted in accordance with reference (a), Article 540.

(1) Each unissued short title of keying material must be verified against the Status of COMSEC Material Report (SCMR) or relevant Record Messages on file. Destruction dates in LCMS do not necessarily reflect the actual destruction date of keying material in all instances.

(2) As the TIER 2 Parent Account, NCTS Guam has five working days to complete routine destruction. LE's must perform destruction within 12-hours of supersession and MUST report destruction to NCTS Guam within three days.

(3) The procedures documenting destruction may be found in enclosure (12) of reference (a).

f. Local Management Device/Key Processor (LMD/KP) Maintenance. Backups and maintenance functions are performed on the LMD/KP at varying intervals from daily (database backups) to every three years (KP Rekey). All non-daily re-occurring tasks shall be scheduled on a calendar and EKMS Office Plan of the Month accessible to all EKMS Personnel according to the following schedule:

- (1) Daily Backups - Daily
- (2) Full Backup Root - Every 30 days
- (3) Full Backup User - Every 30 days
- (4) Change LMD Password - Every 90 days
- (5) Change KP Pin - Every 90 days
- (6) KP Change Over - Every 90 days
- (7) Archive - Every 6 months
- (8) Inventory Reconciliation Status Transaction (IRST) - every 6 months
- (9) KP Rekey - Every 12 Months
- (10) KP Recertification - Every 3 years

(a) The required maintenance for the LMD/KP may be found in reference (a), Articles 718.d, 1005.a.11, and 1185.

(b) Logs of all maintenance will be maintained in accordance with reference (a), Chapter 7.

g. LE Interaction. It is the responsibility of the EKMS manager to ensure a current continual awareness of local and national EKMS Policy/Procedures among all LE's. The EKMS Manager shall conduct monthly spot-checks in accordance with references (a) and (c).

h. Training. The EKMS Manager shall provide LE training on EKMS/COMSEC matters on a monthly basis. Most training will be provided by virtue of computer base training (CBT) via DCO (<https://connect.dco.dod.mil/nctsguamekmstraining/>).

Some training will be in-person to facilitate a better understanding of key topics. Training shall address common and current problems (especially incidents and practices dangerous to security) as well as review proper procedures and best-practices. The EKMS Manager shall maintain a Record of Training binder to include, at a minimum, the date, topic, and attendees.

i. Incidents and Practices Dangerous to Security (PDS).

COMSEC material is sensitive information requiring a positive chain-of-custody and accountability to safeguard tactical, strategic, and national security. The **unreported** loss, theft, or mishandling of COMSEC keying material is among the most serious of security breaches. These incidents **must be reported immediately to avoid further damage**. Reference (a), Chapters 9 and 10, provide detailed information on reporting both COMSEC Incidents and Practices Dangerous to Security (PDS). In addition, the following guidelines will also be followed:

(1) Any loss or compromise of COMSEC material shall be reported immediately to the EKMS Manager who will advise the Commanding Officer and the chain of command immediately.

(2) Reports of any incident must be made in accordance with reference (a), and according to its definitions. If in doubt as to whether an incident has occurred, the report shall be made.

(3) NCTS Guam is responsible for making all incident and PDS reports for all items assigned to account 259015 in accordance with reference (a). While LE commands are required to make reports to NCTS Guam, external reports shall not be delayed if the LE reports are not timely. In those unusual cases, the LE chain of command will be included in the message adders for synchronization of effort.

j. Emergency Action Plan (EAP). The EAP must meet the minimum requirements of reference (a), Annex L, and include procedures for LE involvement. EAP in conjunction with the Emergency Destruction Plan (EDP) drill shall be conducted annually.

9. Responsibilities and Duties: LE Commanding Officer.

a. Unless specifically stated otherwise, the term "LE Commanding Officer" may be interchanged with "Officer in Charge" (OIC) or "Staff CMS Responsibility Officer" (SCMSRO).

b. LE Commanding Officers are responsible and accountable for the management and security of all COMSEC material held by their command and shall ensure compliance with the references, policy, and procedures of this instruction.

c. In accordance with reference (a), Article 420, appoint, in writing, qualified and responsible individuals as the account Local Element Custodian (LEC) and at least one Alternate Local Element Custodian (ALEC), Sub-Local Element Custodian and at least one Sub-Local Element Alternate Custodian, and as many Witnesses as needed to support daily EKMS functions. Commanding Officers should also take into account TAD and extended Leave periods when determining the number of ALEC's and Sub-Local Element Alternate Custodian's.

d. The LEC and Sub-LEC must be at least an E-5 or a GS-5. ALEC's and Alternate Sub-LEC's must be at least an E-5 or GS-5. Witnesses may be assigned at the discretion of the LE CO as long as the witness is authorized access, in writing, to keying material.

e. Personnel must be appointed in writing by the Commanding Officer or by someone acting in his or her stead and authorized to sign official command correspondence as "Acting." (IAW reference (a), "By direction" signature authority is not sufficient for this purpose).

f. Establish, in writing, a list of personnel authorized access to COMSEC keying material in accordance with reference (a), Article 450.

g. Ensure EKMS training is conducted and reported to the EKMS Manager monthly to meet the requirements outlined in reference (a). Where practicable, training should be accomplished with the NCTS Guam EKMS Manager to enhance standardization and best practices.

h. Ensure COMSEC Incidents and Practices Dangerous to Security are reported promptly to NCTS Guam and that corrective actions are taken as required. For incidents and reportable practices dangerous to security as defined in Articles 945 and 1005 of reference (a), reports shall be made via Naval message to NCTS Guam in the format described in reference (a) Article 970 (incidents) or Article 1010 (PDS). As the parent account, NCTS Guam will make all subsequent reports.

i. Ensure local procedures are established for identification and reporting of any potentially significant changes in life-cycle, financial status, or disciplinary problems involving personnel authorized access to COMSEC material; and that those changes are immediately reported to the EKMS Manager and Command Security Manager as appropriate.

j. Ensure account quarterly inspections are conducted where, COMSEC material is used and stored:

(1) The Commanding Officer may delegate 2 of 4 quarterly inspections to the Executive Officer.

(2) Executive Officers must conduct quarterly spot checks. This is in addition to any spot checks performed for the CO.

(3) Department Heads whose divisions or work centers perform COMSEC duties must perform a quarterly spot check on at least one division or work center.

(4) When assigned as the LEC's supervisor, either the Division Officer or Leading Chief must perform a monthly EKMS spot check within the division. The emphasis for these spot checks shall be to ensure the division's documentation is correct and the individuals are following the guidance set forth in COMSEC publications, command instructions, and Standard Operating Procedures in accordance with reference (b).

k. Ensure the local Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP) is established and tested in accordance with reference (a), Annex L.

l. Ensure the inventory of all COMSEC material held is conducted in conjunction with a change in Commanding Officer, change of Local Element Custodian (LEC), semi-annually as required by reference (a), and as directed by the EKMS Manager, NCTS Guam. **Notification to the EKMS Manager is required prior to any of the above change in personnel.**

m. Active involvement by the Commanding Officer in oversight of Local Element operation and management has shown to be a single common factor in preventing major COMSEC incidents and Practice Dangerous to Security (PDS).

n. A biennial Physical Security Survey is required for those local elements holding keying material or classified COMSEC; certification criteria is listed in reference (b).

o. The LE Commanding Officer must review and sign all inventories, quarterly inspections, hand receipts, and destruction reports; hand receipts and destruction reports may be accumulated and signed monthly.

NOTE: Block 17 of the SF-153 is reserved for the Commanding Officer, SCMSRO, or OIC's signature; refer to reference (a), Annex T.

10. Local Element Custodian (LEC).

a. The LEC is responsible for the proper day-to-day management and security of all COMSEC material held at the LE. LEC's also serve as the Commanding Officers primary advisor on EKMS matters. In this capacity the LEC as well as the ALECs, share equally the following duties:

(1) LECs are responsible to the Commanding Officer for proper management and security of COMSEC material held by the command. LEC's are also responsible to the EKMS Manager for the proper accountability, security, control, and disposition of COMSEC material issued to them.

(2) LECs must provide their Commanding Officer with information about new or revised COMSEC policies and procedures and their impact on the command.

(3) LECs are responsible for providing guidance concerning handling, accountability, and disposition of COMSEC material to all LE personnel. LEC's must conduct monthly training to ensure that all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures with emphasis on accountability, security, Two Person Integrity (TPI) requirements, and the identification of improper practices. This training must be documented and records maintained locally.

b. Ensure proper storage and adequate physical security is maintained for COMSEC material.

c. Complete, maintain, and forward required accounting records and reports (i.e. destructions reports) to the EKMS Manager within the time limits given per reference (a).

(1) Report the following to NCTS Guam EKMS Office:

(a) Monthly destruction no later than the 2nd working day of the month (Original SF-153 and CMS-25 forms).

(b) Pre-draw request no later than the 10th of each month. No earlier than 30 days from effective date of use.

(c) Scheduled monthly DTD/SKL audit trail review

(d) Weekly DTD/SKL inspection to detect any breach in the casing (Report as Physical Incident if any cracks or breaches are detected).

(e) EKMS training report no later than the 25th of each month.

(f) LE Commanding Officer/OIC EKMS Spot Check result no later than the 30th day of the month.

(g) EDP Drill report no later than the 25th of the months of March, June, September and December.

(h) STE quarterly report no later than the 25th of the months of March, June, September and December.

(i) Semi-annual Inventory Report (SAIR) no later than the 25th of the months of April and October and When Directed (WHENDI).

(j) EAP in conjunction with EDP drill shall be conducted no later than the 25th of the month of March annually.

d. The LEC will maintain a LE Chronological File, LE Correspondence file, LE Directives file, LE Local Custody file and a LE Message File in accordance with reference (a), Chapter Seven.

e. In accordance with reference (a), Annex T, ensure two appropriately cleared personnel sign all SF-153s; this will normally be the LEC and ALEC, or one Custodian and one cleared person identified as a witness in accordance with reference (a), Article 440.h.

f. Ensures adherence to TPI requirements.

g. Report immediately any known or suspected PDS or COMSEC incident to the LE Commanding Officer, EKMS Manager, and NCTS Guam. Coordinate with the EKMS Manager to ensure the required reports are submitted, and when required, replacement material is obtained.

h. Ensure that the LE does not receive or transfer COMSEC material from/to an EKMS account other than NCTS Guam in accordance with reference (a).

i. Personnel designated to transport COMSEC material must possess a Courier Authorization Card (DD Form 2501).

j. Appoint a new LE Primary or Alternate Custodian if the current Primary or Alternate Custodian is away due to Permanent Change of Station, Leave, and TAD/TDY in excess of 30 days.

k. Unrestricted access to Supervisory Crypto Ignition Keys (CIKs) for DTD and Site Security Officer (SSO) password for SKL must be limited only to personnel who are authorized in writing to perform all of the associated privileges.

l. Ensure that the LE personnel have been SCI Indoctrinated if material is held/used for Sensitive compartmented information/ Special Intelligence (SCI/SI) circuits.

11. Return/Transfer of Equipment.

a. Return of COMSEC. In the event the LE wishes to be relieved of accountability and return any equipment, provide written documentation to the EKMS Manager at (M-GU-NCTSGUAMEKMS@fe.navy.mil) with the following information:

(1) Type of equipment they wish to return (i.e., KIV-7, KG-175, etc).

(2) Quantity and serial numbers.

(3) Reason Statement: "Equipment is no longer required because (i.e., circuit is no longer in use). "Please note if equipment is not operable!"

b. Transfer of COMSEC. COMSEC may not be transferred / "sub-custodied" to another command, except by NCTS Guam. Commands designated as "Issuing LEs" may only issue to the Sub-LE's (detachments, boat units).

12. Responsibilities and Duties: EKMS Users. Whether EKMS Users personally sign for COMSEC material on local custody or are using COMSEC material signed for by someone else (e.g., a watch supervisor), they are responsible for the proper security, control accountability, disposition or destruction of the material. An EKMS user must comply with applicable security, control, and internal accountability procedures outlined in reference (a) and this instruction.

13. Safeguarding COMSEC Material and Facilities. Each person involved in the use or storage of COMSEC material is personally responsible safeguarding the material, properly using the material for which they are responsible, and promptly reporting to proper authorities any occurrence, circumstance, or act which could jeopardize the security of COMSEC material.

a. Only cleared persons with a valid need-to-know shall have access to COMSEC.

b. Contractor personnel with a valid need, and when it is clearly in the best interest of the DON and the U.S. Government, may have access to COMSEC equipment, keying material (including manual COMSEC systems), related COMSEC information, and access to classified U.S. Government information in accordance with reference (a), Article 505(f).

14. Inventories. All inventories will be conducted in accordance with reference (a), Article 766

a. Specifically, the following events require an inventory:

- (1) Change of Command at NCTS Guam
- (2) Change of Command at a LE
- (3) Change of EKMS Manager, NCTS Guam
- (4) Change of LE Primary Custodian
- (5) Unit Disestablishment
- (6) Semi-Annual Inventory (April and October)
- (7) When Directed (WHENDI)

b. When an inventory is required, issuing LE's shall collect, consolidate and retain written documentation of sight inventories for COMSEC assigned to detachment / remote personnel in accordance with reference (a), Annex S. Detachments should submit a signed inventory via fax, scan, mail, or by record message to the LE. The LEC will forward LE and detachment inventories to the EKMS manager for consolidation and account records.

c. Watch Station Inventories. Each watch section supervisor is responsible for all COMSEC material listed on the watch-to-watch inventory. An inventory of all COMSEC material and SF-700's will be held by two cleared EKMS User PQS 301 qualified personnel; one from the oncoming and one from the off-going watch section, prior to assuming the watch. This inventory will include sighting the watch-to-watch inventory and the CMS-25 local destruction report against the actual material. The inventory will be completed in accordance with enclosure (13).

15. Amendments. Amendments to COMSEC publications will be entered in accordance with reference (a), Article 787 to document amendment entries, verification and residue.

16. Over-The-Air Transfer/Over-The-Air-Rekey (OTAT/OTAR). Procedures and policies for training and conducting OTAT/OTAR are contained in references (c) and (d); NCTS Guam specific OTAR/OTAT procedures are listed in enclosure (12). All LE accounts conducting OTAT/OTAR must maintain and become familiar with both references. They are part of the required reading and have been incorporated into the EKMS training program (watch station JQR and PQS).

17. Disposition and Destruction of COMSEC Material.

a. Local Destruction Procedures. Local destruction of COMSEC material will be accomplished in accordance with reference (a), Article 540 and the following:

(1) As the Parent Account, NCTS Guam must finalize all destruction reports to include signatures by the EKMS Manager, the witness, and the Commanding Officer within five (5) working days from the first working day of any given month.

(2) To meet that requirement, all Local Elements will perform destruction within 12 hours of supersession and will

26 Jun 15

submit their destruction SF-153 reports to the EKMS Manager, NCTS Guam within three (3) working days. Exceptions to the 12 hour rule may be found in reference (a), Article 540.e.

b. Disposition Procedures. All COMSEC material must be disposed of in accordance with the directions provided by higher authority. LE's shall turn in any CCI no longer in use to the EKMS manager for redistribution or destruction.

(1) In the interest of maintaining communications security and a high state of operational readiness, COMSEC material must never be used before it is authorized for use and must never be destroyed before it is authorized for destruction; in regards to EKMS material, the authorized use date is referred to as the "effective" date. A material's authorized destruction date is referred to as its "supersession" date. Both effective and supersession dates of a COMSEC material item are referred to collectively as the material's status.

(2) With the exception of COMSEC equipment, almost all COMSEC material is assigned effective and supersession dates. The LE's will receive the effective and supersession dates from the NCTS GUAM EKMS Manager. The Manager will advise all LEC's of the status of material issued to them.

NOTE: When a short title and its supersession date are documented together, the document becomes CONFIDENTIAL and must be protected as such. EKMS forms which have been used to document the destruction of keying material will be classified CONFIDENTIAL.

(3) LEs are authorized to conduct monthly destructions utilizing CMS-25 derived from reference (a), and verification of supersession will come from the EKMS Manager, by using the Status of COMSEC Material Report (SCMR) or Record Message traffic. The messages will be released by the controlling authority and the EKMS Manager will provide the message to the LE's. The CMS-25 must be returned to the EKMS Manager along with the signed SF-153 destruction report.

(4) Unissued COMSEC Keying Material. The destruction of unissued COMSEC keying material must be conducted by the EKMS Manager/Alternate and a properly cleared/qualified witness. Destruction must be made by the EKMS Manager and the EKMS Manager Alternate or by the EKMS Manager Alternate and a properly cleared witness.

26 Jun 15

c. Issued COMSEC Keying Material. The destruction of issued COMSEC keying material must be conducted by two EKMS PQS qualified and properly cleared personnel. Personnel having local custody responsibility for issued material and a witness are authorized to destroy the keying material. The witness will be an EKMS 301 PQS qualified U.S. military or civilian employee who possesses a security clearance equal to or higher than the classification of the material being destroyed. The witness must receive instruction on EKMS destruction procedures prior to witnessing destruction. One of the two individuals must be, at a minimum, E-5 or GS-5 equivalent.

d. Destruction Procedures. The individuals conducting EKMS destruction will comply with the guidelines of reference (a), Article 540, and the following:

(1) Individual segments must be verified, destroyed, and documented separately. Under no circumstances will COMSEC material be "group verified and group destroyed, TPI members may NOT be relieved or replaced before the destruction process is complete.

(2) Destruction of entire editions. Whether routine or emergency supersession occurs, a destruction record (SF-153) may document the date of destruction for a complete edition of material. After the LE Custodian verifies destruction by checking each CMS-25 for the dates, signatures/initials, short title, edition, register number and AL code, submit the SF-153 and CMS-25 destruction forms as follows:

(a) Original to EKMS Manager.

(b) Copy to the LE Custodian.

(3) Destruction of individual segment. CMS-25 forms will be used to document the destruction of extracted segments from a DTD/SKL or Canister (paper tape).

(a) CMS-25 forms will list the following:

1. LE account identification/name
2. CONFIDENTIAL (When filled in) marking
3. Short title, registration/serial number / unique variable, AL code, classification and edition.
4. HJ time

5. Circuit/usage
6. Segment effective status
7. Edition status
8. Classification
9. Derived from: EKMS 1(Series)
10. Declassify on: 22 SEP 2028

(b) The EKMS Manager will verify completeness of the CMS-25 against the SF-153. Upon completion of verification, the EKMS Manager is authorized to destroy the CMS-25 destruction forms.

NOTE: On CMS-25 forms, a line must be drawn diagonally from the last segment destroyed to the last number on the form and a statement "Nothing Follows" must be placed on the line. Both individuals conducting the destruction will place their signatures and date upon the line.

(4) Each person involved in the destruction is equally responsible for the timely and proper destruction of the material and for accuracy of the destruction records. The material must be destroyed as soon as possible or within twelve hours after.

(5) Acceptable Writing Instruments. Only black ball point pens are authorized for use on any EKMS destruction, inventory, transfer, receipt reports or any EKMS related document.

e. Emergency Supersession of Keying Material. Emergency destruction of material which has been subject to compromise will be conducted in accordance with reference (a), Article 540. Emergency supersession destruction will be directed by Record Message and a copy will be provided to any Local Element possessing compromised keying material. Destruction due to emergency supersession must occur within 12 hours of notification and the supporting documentation must be returned to NCTS EKMS Office immediately upon completion.

NOTE: Destruction of emergency superseded keying material will be coordinated by the EKMS Manager.

18. COMSEC Incidents and Practices Dangerous to Security (PDS) Reporting Requirements.

a. COMSEC incidents, as defined by reference (a), Chapter Nine, must be immediately reported to the EKMS Manager, NCTS Guam. Any delay in reporting a COMSEC incident could result in serious damage to National Security.

b. PDS, as defined by reference (a), Chapter 10, while not reportable to the national level National Security Agency (NSA), are practices which have the potential to jeopardize the security of COMSEC material, if allowed to perpetuate, could lead to a COMSEC Incident. Promptly report known PDS to the EKMS Manager, NCTS Guam so corrective measures may be taken.

19. Data Transfer Device (DTD) and Simple Key Loader (SKL). The DTD/SKL is used to securely distribute key generated by the LMD/KP to an End Cryptographic Unit (ECU) or when authorized, to another DTD/SKL. The DTD/SKL is also able to replace current common fill devices (FD's) such as the KYK-13 or KYX-15.

20. Introduction to the Secure Terminal Equipment (STE). The information provided below gives a brief description of the STE and the associated KSV-21 card.

a. Secure Terminal Equipment. The STE is the new generation of secure voice and data equipment designed for use on advanced digital communications networks, such as Integrated Services Digital Network (ISDN) and Public Telephone Switched Network (PTSN). The STE consists of a host terminal, that is NOT CCI, but to be handled as a high cost government item. It has a removable security core. The host terminal provides the application hardware and software. The security core is the KSV-21 cryptographic card that provides all the security services.

b. KSV-21 card. The KSV-21 is a high-grade security token with built-in U.S. Government-owned encryption algorithms and public key exchange protocols. Before the KSV-21 card can be used, the cryptographic keys must be programmed and stored in the card by the EKMS Manager. The KSV-21 card is built with many anti-tamper technologies, one of which is the Crypto Ignition Key (CIK).

(1) When inserted in a STE, the KSV-21 STE system is classified and must be protected to the highest security level

26 Jun 15

associated with the classification level of the KSV-21. A User may insert the KSV-21 card in the STE at the beginning of the day and leave the card in place as long as an authorized User is always present to maintain positive control of the KSV-21 and STE.

(2) With appropriate cryptographic keying material in the KSV-21 card, the combination of KSV-21 and STE has been approved to protect U.S. Government information up to and including TOP SECRET/Sensitive Compartmented Information (TS/SCI). Moreover, the STE is approved for installation in Sensitive Compartmented Information Facilities or SCIF's.

c. STE/KSV-21 User Responsibilities and Storage.

(1) A User who accepts the use of a KSV-21 card is solely responsible for safeguarding the card and cannot transfer the card without approval from the EKMS Manager. A User may allow or permit others to use his or her card as long as the person is cleared to the security level of the keys programmed on the card.

(2) An authorized User must supervise access by a person not having an appropriate clearance to a STE.

(3) A User must protect a KSV-21 card by either keeping it in the User's personal possession or storing it in a manner consistent with the classification level the KSV-21 and STE combination may attain.

(4) When not in use, the KSV-21 must be stored in a secure area and an approved GSA container (safe).

(5) Each assigned User must complete a COMSEC Responsibility Acknowledgement Form (enclosure (2)) or STE Statement of Responsibility Form (enclosure (3)) to facilitate the tracking and accountability of each KSV-21.

(6) STEs must be re-keyed at regular intervals, if not completed the STE will function in the UNCLASS mode ONLY. Compliance with NCTS Guam STE re-key requests will ensure the STE maintains full functionality.

21. Emergency Action Plan (EAP). The Command's EAP must address COMSEC Material. In addition to the procedures for the execution of an EAP at NCTS Guam, the EAP must address

coordination with Local Elements, including detachments, external to NCTS Guam. The minimum requirements for an EAP are listed in reference (a), Annex L.

a. EAP Drill. A simulated execution and documentation of the EAP in conjunction with EDP at NCTS Guam and its LE's must be conducted annually.

b. EDP Drill. A simulated execution and documentation of the EDP at NCTS Guam and its LEs must be conducted quarterly.

22. Notification. The EKMS Manager or Alternate Manager(s) and the Local Element CO will be notified immediately when the following occurred:

a. Inadvertent extraction and destruction of keying material (KEYMAT).

b. When adjusting over-the-air rekeying (OTAR) Traffic Encryption Key (TEK), Non-OTAR TEK and OTAR KEK to the next segment as a result of bad load or accidental zeroization of the keymat.

c. When COMSEC Incident and PDS have been committed.

NOTE: The information provided must be of sufficient detail to enable NCTS Guam to assume responsibility for reporting the incident.

NCTSGUAMINST 2280.1U
N00SM
26 Jun 15

SAMPLE LETTER OF APPOINTMENT

2200
Ser N1/
DD Mmm YY

From: Commanding Officer or Officer-in-Charge, (Command Name)
To: Rank/Rate First MI. Last, CIV

Subj: LETTER OF APPOINTMENT AS (COMMAND NAME) LOCAL ELEMENT
PRIMARY OR ALTERNATE CUSTODIAN

Ref: (a) EKMS 1 (Series)

1. Per reference (a), you are hereby appointed as EKMS Local Element Primary or Alternate Custodian for (Command Name).
2. Under CMS Parent account number: 259015
3. EKMS 302 PQS completed on: 01 JAN 2011
4. Security clearance: Secret
5. Following designation requirements contained in Article 412 of reference (a) are waived: Not Applicable.

I. M. COMMANDING

Copy to:
NCTS Guam EKMS Manager
LE Correspondence File

Enclosure (2)

CRYPTOGRAPHIC ACCESS CERTIFICATION AND TERMINATION			
PRIVACY ACT STATEMENT			
<p>AUTHORITY: EO 9397, EO 12333, and EO 12356. PRINCIPAL PURPOSE(S): To identify the individual when necessary to certify access to classified cryptographic information. ROUTINE USE(S): None. DISCLOSURE: Voluntary; however, failure to provide complete information may delay certification and, in some cases, prevent original access to classified cryptographic information.</p>			
INSTRUCTIONS			
<p>Section I of this certification must be executed before an individual may be granted access to classified cryptographic information.</p> <p>Section II will be executed when the individual no longer requires such access.</p> <p>Until cryptographic access is terminated and Section II is completed, the cryptographic access granting official shall maintain the certificate in a legal file system, which will permit expeditious retrieval. Further retention of the certificate will be as specified by the DoD Component record schedules.</p>			
SECTION I - AUTHORIZATION FOR ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION			
<p>a. I understand that I am being granted access to classified cryptographic information. I understand that my being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.</p> <p>b. I understand that safeguarding classified cryptographic information is of the utmost importance and that the loss or compromise of such information could cause serious or exceptionally grave damage to the national security of the United States. I understand that I am obligated to protect classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions, issued by my department or agency, regarding unofficial foreign travel or contacts with foreign nationals.</p> <p>c. I acknowledge that I may be subject to a non-lifestyle, counterintelligence scope polygraph examination to be administered in accordance with DoD Directive 5210.48 and applicable law.</p> <p>d. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793, 794, 798, and 952. I understand that, if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate. I understand and accept that unless I am released in writing by an authorized representative of <i>(insert appropriate security office)</i>, the terms of this certificate and my obligation to protect all classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.</p>			
<p style="text-align: center;">ACCESS GRANTED THIS _____ DAY OF _____, _____</p>			
1. EMPLOYEE			
a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE/RANK/RATING	d. SSN
2. ADMINISTERING OFFICIAL			
a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE	d. OFFICIAL POSITION
SECTION II - TERMINATION OF ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION			
<p>I am aware that my authorization for access to classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any classified cryptographic information I acquired, nor discuss with any person any of the classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952; and Title 50, United States Code, Section 783(b).</p>			
<p style="text-align: center;">ACCESS WITHDRAWN THIS _____ DAY OF _____, _____</p>			
3. EMPLOYEE			
a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE/RANK/RATING	d. SSN
4. ADMINISTERING OFFICIAL			
a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE	d. OFFICIAL POSITION

26 Jun 15

STE STATEMENT OF RESPONSIBILITY SHEET
(Print as two-sided to keep all signatures with Statements)
EKMS Account 259015
STE/KSV-21 Holder Listing

Name: _____ Rank: _____ Command: _____

Clearance: _____ Location: _____ Phone: _____

Office Code: _____ Date: _____

ITEM	KSV21 S/N	ALC	QTY	TYPE	CARD	¹	²	³	STE TERMINAL S/N
1	259820	1	1	1					STEA3000123456

Statement of Responsibility

The above KSV-21 listing corresponds to the KSV-21 cards that have been issued to you. Each KSV-21 is a COMSEC material continuously accountable to the COR by accounting by serial number from production to destruction. You must institute local controls limiting access to the keyed Terminal (KSV-21 inserted) to those persons who have appropriate Security Clearance and Need-To-Know. The STE terminal, when unkeyed (KSV-21 removed), is an UNCLASSIFIED high value property item.

The secure mode should be utilized whenever possible during conversations with another STE Terminal user. You must not exceed the classification level displayed in the terminal. The classification displayed is the highest Security Clearance common to both parties in any given call. The classification displayed may be equal to or lower than your own.

The KSV-21 must be removed from the terminal, kept in your possession and protected as high value personal property after normal working hours. Do not leave the KSV-21 unattended in the STE. The only exception to this are those STEs used for gateway connectivity for communications (e.g., message traffic) purposes utilizing the SACS mode of operation. If the KSV-21 is stored in the vicinity of the terminal it's associated to, it must be secured in a GSA-approved security container.

If a KSV-21 is lost, stolen, or misplaced, you must notify your EKMS Manager/STE MC User immediately so that compromise recovery/prevention measures can be taken. The EKMS Manager/STE

26 Jun 15

MC User may be reached by phone during normal working hours at (671) 355-5887. After hours, contact the EKMS Manager at (671) 688-3497 or NCTS Guam CDO at (671) 688-3497. I, the person whose signature appears below, certify that I have in my possession and hold myself responsible for the STE material listed above, commencing on the date indicated, and that I understand the requirements for safeguarding the same.

I have read and accept the responsibilities stated above:

Signed: _____ Date: _____

¹ = TPA Card

² = User Card.

³ = Carry Card

⁴ = Optional, but highly recommended.

The EKMS Manager/STE MC User may be reached by phone during normal working hours at (671) 355-5888/5887. After working hours contact the Command Duty Officer at (671) 688-3497.

COMSEC MATERIAL REQUIRED READING LIST

1. The publications, chapters and articles listed below constitute the required reading for NCTS GUAM EKMS. This list will be read by all qualified EKMS Users and those under Department/Division training personnel incorporate these requirements into their regularly scheduled monthly training plan. More frequent light reading assignments on a regular monthly basis will have greater impact than will less frequent heavy reading assignments.

EKMS 1 (SERIES)

<u>Chapter/Article</u>	<u>Subject</u>
Chapter 1:	Communications Security (COMSEC) Material Control System (CMCS)
Chapter 2:	Introduction to COMSEC Material
Chapter 3:	EKMS Education, Training, and Inspections
Chapter 4:	Establishing a EKMS Account and Responsibilities
Chapter 5:	Safeguarding COMSEC Material and Facilities
505-510:	Access and Release Requirements for COMSEC Material/Two Person Integrity (TPI) Requirements
515:	Access to and Protection of Safe Combinations
520:	Storage Requirements
535:	Controlled Cryptographic Item (CCI)
540:	General Routine Destruction Guidance
545-550:	COMSEC Facilities/Safeguarding Fixed COMSEC Facilities
570-575:	Safeguarding Transportable and Mobile COMSEC Facilities/Safeguarding DOD Black Bulk Facilities

Chapter 6:	Maintaining COMSEC Material Allowance
601:	General
620:	Maintaining Reserve-On-Board (ROB) Level of Keying Material
630:	Defense Courier Service (DCS)
670:	Requesting Electronic Keying Material
Chapter 7:	COMSEC Documentation Requirements for COMSEC Material
775:	COMSEC Material Management in a Watch Station Environment
787:	Entering Amendments and Corrections to COMSEC Publications
790:	Procedures for Destroying COMSEC Material in Paper Form
Chapter 8:	Disestablishment of an EKMS Account
Chapter 9:	COMSEC Incident Reporting
Chapter 10:	Practices Dangerous to Security (PDS)
Chapter 11:	Management of Electronic Key

NCTSGUAMINST 2280.1U

N00SM

26 Jun 15

ELECTRONIC KEY MANAGEMENT SYSTEM LOCAL ELEMENT TRAINING

1. The EKMS PQS 301(users) & 302 (LE custodians) training is required in accordance with EKMS 1B(series).
2. Required monthly training will be conducted and archived at (P:\N00SM\N00SM4_EKMS\2015_EKMS\Training) for missed attendance and self-refresher.

NCTSGUAMINST 2280.1U

N00SM

26 Jun 15

AUDIT TEAMS COMMAND PERIODIC REVIEW CHECK LIST

1. This enclosure is located on the NCTS Guam Public Share (P:\N00SM\N00SM4_EKMS\2015_EKMS\COMSEC Library). A hard copy of the EKMS 3D is located in the Guam EKMS Manager office.

NCTSGUAMINST 2280.1U
 N00SM
 26 Jun 15

CONFIDENTIAL (WHEN FILLED IN)
EKT/OTAT KEY GENERATION LOG
 (FILL IN COMPLETELY BEFORE STARTING NEW LOG)

OPEN DATE: _____ CLOSE OUT DATE: _____

.....

XMT/ RCV CKT OCTAL	KEY ID SHORT TITLE	S E G	C L A S S	P E R	EFF DTG	SPRCDED DTG	FD/P8N SERIAL#	PURPOSE (USE)	DATE RCVD	XMT STN	RCV STN	CSE SUP	CSE OPR	ZEROIZED DTG	CSE SUP	CSE OPR

DERIVED FROM: EKMS 1 (SERIES)
 DECLASSIFY ON: 22 SEP 2028
 REVIEWED BY: _____ DATE: _____

"RETAIN FOR 60 DAYS BEYOND CLOSE OUT DATE IAW EKMS 1 SERIES
 ANNEX T"

CONFIDENTIAL (WHEN FILLED IN)

DATA TRANSFER DEVICE USER GUIDE (AN/CYZ 10)

1. The Data Transfer Device (DTD) has a host side and a crypto side. The host side is a small computer used to control the functions of the DTD or run User Application Software (UAS) (e.g., Card loader UAS (CLUAS) and Common UAS (CUAS) for special functions. The crypto side performs the cryptographic functions.

2. The DTD is powered by three 3V lithium batteries (Duracell Type DL123A, NSN 6135-01-351-1131). Use only the fused battery holder (ON 4767435-2). This fused battery holder requires replacement in the event of a blown fuse. A standard 9V Duracell battery may be used if Type DL123A battery is not available.

WARNING: The following battery types will NOT be used in the DTD: Mercury batteries designated BA 1372/U and lithium batteries designated BA 5372/U. Use of these batteries has proven extremely hazardous and has resulted in combustion. The EKMS Manager is not the source of supply for batteries; LEs are responsible for replacing the battery in the DTD(s) issued to their LE. You are encouraged to check your batteries on a regular basis and have spares on hand. In the event the batteries do expire, all association of CIK's and key will be lost. DTDs that receive required monthly reviews very seldom encounter unexpected battery failure.

3. The DTD provides cryptographic security for the storage and transfer of all types of key and protective storage for related data (key tags, audit data, and application software). The key storage capability of the DTD is limited to 1000 individual 128 bit keys. Due to the various sizes (beyond 128 bit) of Modern Key the key storage capability will be no more than 11.

4. The DTD can securely store all classifications and categories on the crypto side. **WARNING:** Electronic key must not be stored on the **HOST** side.

5. The DTD is accountable to the COR as AL Code 1 (by serial number) material.

6. The CIK is locally accountable to the EKMS Manager by assigned serial number. The CIK serial number will be composed of the last four digits of the associated DTD serial number, followed by '01' for the EKMS Manager's Supervisory CIK, '02'

for the Supervisory User's CIK, or '03' through '08' for the User CIK's.

7. The DTD is unclassified CCI until:

a. Key is loaded on the crypto side, and the CIK is inserted, handling requirements shall be maintained IAW the classification level of the resident key. When the CIK is not inserted the DTD is unclassified. A tag will be attached to each DTD, via the lanyard ring, that indicates the classification of the DTD when its associated CIK is not inserted. Tag will read as follows:

"This device is classified up to the level of keying Material stored within. TPI is required if TS material is held. This device becomes unclassified when either the DTD, or it's associated CIK(s) are stored separately, in a container without single person access."

8. CIK Classification and Handling.

a. The CIK itself is unclassified. The CIK shall be stored separately from the DTD/SKL. With the CIK inserted, the key stored within is accessible and the DTD/SKL shall be classified at the highest level of key stored therein.

b. When inserted, the CIK is classified to the highest level of unencrypted key it can output from the DTD/SKL. The CIK will retain that classification until the key is zeroized from the DTD/SKL.

c. A CIK can output only encrypted key from the DTD/SKL and is unclassified, providing the TrKEK used to pre-encrypt the key is inaccessible to Users.

d. A tag must be attached to the CIK via a lanyard to identify the CIK's highest classification level and serial number.

9. TPI Requirements.

a. CIKs that allow output of unencrypted TOP SECRET key designated CRYPTO requires TPI handling and storage. When authorized Users are not present, a TOP SECRET CIK must be removed from the DTD/SKL and returned to TPI storage or **both** CIK and DTD/SKL must be continually safeguarded according to TPI

rules. When TPI storage is limited, and it is necessary to store more than one TOP SECRET CIK in a single TPI container, each CIK shall be individually sealed in its own envelope, the signatures of two individuals authorized access recorded along the seams, and the seams taped shut with cellophane tape. Additionally, the CIK's classification and serial number shall be recorded on the outside of each envelope.

10. DTD/SKL CIK Clearance and Access Requirements.

a. Formally designated access is not required for external viewing of a CIK (Supervisory or User, classified or unclassified) or a DTD/SKL that does not contain a key or data, nor is a clearance required for external viewing of an un-keyed DTD/SKL containing classified key designated CRYPTO or data. Unrestricted access to a DTD/SKL or to a CIK associated with a DTD/SKL containing the keying material requires a clearance equal to the highest classification indicator of the keying material. Unrestricted access to a DTD/SKL keyed with a classified CIK or to a classified CIK also requires written access authorization. Unrestricted access to a Supervisory CIK must be limited to individuals authorized to perform all of the privileges allowed by the Supervisory CIK.

11. Storage of Key in the DTD/SKL.

a. No more than one canister of keying material (per short title), not to exceed twelve months and one spare month of keying material shall be held in a DTD/SKL at any time. The only exception to the "one canister" rule per DTD/SKL is that the follow-on canister of keying material can be loaded into the DTD/SKL at any given time during the final month prior to the current edition being superseded. There is no limitation on the length of time that User key may be stored in the DTD/SKL, however, superseded key must be destroyed in accordance with proper guidance. (See below). **Warning:** Key will **not** be stored on the DTD/SKL host side.

12. Destruction of Key in DTD/SKL.

a. Destroy/delete emergency superseded key as soon as possible and always within **12 hours** of receipt of emergency supersession notification.

- (1) Users may postpone destruction of superseded

segments until the entire edition is superseded or until the next use of the DTD/SKL, whichever occurs first. If superseded segments are retained until the edition is superseded, they must be destroyed no later than 12 hours after the entire edition is superseded.

(2) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hour standard (i.e., operational space not occupied), destruction may be postponed until the next duty day. In such cases, the material must be destroyed as soon as possible after reporting for duty.

b. Irregular supersession promulgated by message must be destroyed as soon as possible after receipt of the supersession message and always within 12 hours of receipt.

c. Failure to zeroize superseded electronic key from the DTD/SKL in the specified time, is a non-reportable PDS. A non-reportable PDS is however reportable to the LE Commanding Officer. The signed original is filed in the LE Correspondence File.

13. Transportation Requirements.

a. Shipping the DTD/SKL

(1) The DTD/SKL must always be shipped separately from its associated CIK(s) once the CIK(s) are initialized. Approval is required by the EKMS Manager.

(2) When the DTD/SKL contains no keying material and no classified host side data, transport using any of the means approved for UNCLAS CCI.

b. Shipping the CIK

(1) The CIK must be shipped separately from its associated DTD/SKL, using any means approved for keying material of its classification.

c. Hand Carrying the DTD/SKL and CIK(s)

(1) Personnel authorized unrestricted access to a DTD/SKL and its corresponding CIK may be authorized to hand carry the DTD/SKL and CIK, as necessary.

26 Jun 15

The DTD/SKL and corresponding CIK must be appropriately packaged and protected separately from each other (e.g., in a separate container or on the LE courier's person). TPI handling of the CIK will be required when the local command couriers will be simultaneously hand carrying the DTD/SKL and TOP SECRET CIK or when the local couriers will be simultaneously hand carrying the DTD/SKL and CIK and the TrKEK used to pre-encrypt the TOP SECRET key (designated CRYPTO) in the DTD/SKL.

(2) A Courier Authorization Card (DD Form 2501) is required when hand carrying classified material outside of a secure area. Courier Authorization Cards are issued by the Command Security Manager.

14. Audit Trail Record Review Requirements. Local Elements are required to submit all DTD/SKLs that are in their possession to the EKMS Manager every month for the audit trail review and reset. If the DTD/SKL indicates a full data base it must be brought in immediately to the EKMS Manager for audit.

15. DTD/SKL Zeroization and Sanitization.

a. When activated, the DTD/SKL zeroization function will sanitize all data, and destroy all stored keymat. (The zeroize function will not delete application software from the DTD/SKL, nor will it delete audit records from the DTD/SKL).

b. Regardless of its handling requirement before zeroize, once the zeroize function is successfully completed, the DTD/SKL is UNCLASSIFIED CCI. The operator can only treat the DTD/SKL as zeroize if the display shows the "zeroize complete" message. If this message does not appear, a depleted battery may be the cause. Install fresh batteries and press the (zero) key the correct number of times to verify that the display message "zeroize complete" appears. If the message still does not appear, then it must be assumed that zeroize is not possible due to a malfunction. The batteries must be removed from the DTD/SKL and the DTD/SKL must be protected according to its classification, until it can be turned in to a depot and repaired.

NOTE: There is a selective delete function on the DTD Utility menu that may be used for maintaining the accountability of the key. The delete function will not sanitize the DTD or reduce handling requirements of the CIK.

16. Operator Responsibilities.

a. Whenever a CIK fails to work in its intended DTD/SKL, promptly notify the EKMS Manager. He or she will check the update counts of the CIK and DTD/SKL to determine whether or not a review of audit trail records is required.

b. Promptly notify the EKMS Manager of any DTD/SKL's storing key and CIK's that are not properly tagged with the classification and serial number.

c. Familiarize with the handling and safeguarding requirements of EKMS 1B and this Order. Report all violations of same to the EKMS Manager.

d. LE is responsible for periodically checking their DTD/SKL to ensure the battery is not low. Again, it is the responsibility of the LE to purchase and install batteries into their DTD/SKL to ensure the DTD/SKL does not become zeroized.

17. Emergency Protection. Follow the provisions of Annex L of EKMS 1B for the emergency protection of the material in this document. To destroy the DTD/SKL beyond reuse during emergencies (e.g., impending site overrun and capture), where the alternative is possible compromise of the DTD/SKL and the key or data it protects, zeroize the DTD/SKL and smash with fire ax, hammer, or other heavy object.

18. Reportable DTD/SKL COMSEC Incidents.

a. The following are incidents specific to the DTD/SKL.

(1) Loss of a DTD/SKL or a CIK (reportable to the EKMS Manager and the CONAUTH of the key).

(2) Unauthorized access to a CIK or DTD/SKL.

(3) Unauthorized copying of a valid CIK. (i.e., compromise of key as a result of an adversary gaining unaccompanied access to and surreptitiously copying a valid CIK, which can be later used in the associated DTD/SKL before the original CIK is used).

(4) Storage of key on the host side of the DTD/SKL.

(5) Loss of TEMPEST integrity because of failure to detect a breach in the DTD/SKL housing.

(6) Report to the EKMS Manager any of the above.

(7) In the event of Compromise of a lost CIK or DTD/SKL, report promptly to the EKMS Manager.

19. DTD/SKL Repair and Maintenance Users or other authorized personnel may perform only limited maintenance on the DTD/SKL. Limited maintenance, as it applies to the DTD/SKL, is defined as keypad and battery replacement. Personnel replacing these parts are not required to be Qualified Maintenance Technicians.

DESTRUCTION PROCEDURES

1. Verify the supersession date and accounting data of the material to be destroyed.

a. The first individual must hold the material and read the short title and accounting data of the material while the second individual verifies the accuracy and completeness of the entry against the destruction report. Then the material is handed to the second individual.

b. The second individual will then hold the material and read the short title and accounting data of the material while the first individual verifies the accuracy and completeness of the entry against the destruction report. Once both individuals are positive the information is correct -- then and only then -- will they destroy the material.

2. Each will observe the actual destruction of the material.

3. The method of destruction (shred, burn, pulp...etc.) must be in accordance with reference (a), Article 540(j).

4. After the material has been destroyed, each will sign and date the destruction record.

5. Individual segments must be verified, destroyed, and documented separately. Under no circumstances will COMSEC material be "group verified and group destroyed", TPI members may NOT be relieved or replaced before the destruction process is complete.

6. When destroying the key segments in a canister ensure the appropriate "EXTRACTION DATE", TWO SIGNATURES of the individuals for each segment, and the DATE of the destruction are recorded on the CMS-25. Key segments will be removed from the canister when superseded. Once all key tape is removed, puncture empty key tape canisters on both sides of the canister allowing full view of the contents of the canister. Dispose of it as unclassified material. Ensure that the canister is empty before disposing of it.

7. The Local Element Custodian will document the destruction of COMSEC material by entering his/her signature along with and the signature of a qualified witness, and the date on the CMS-25 for

each key segment. If complete destruction of an edition occurs, complete the CMS-25 for each segment, ensuring the signing and dating of all blocks and attach the CMS-25 to the SF-153 Destruction Report provided by NCTS Guam.

CMS-25

Segment	Extracted	Signature	Signature	Destruction Date
01	01/01/2011			02/01/2011

SF-153

SIGN	RANK E-7	SIGN	RANK GS-8
PRINT JOHN DOE	SERVICE USN	PRINT DOE JOHN	SERVICE DOD

8. Each person involved in the destruction is equally responsible for the timely and proper destruction of the material and for accuracy of the destruction records. The material must be destroyed within twelve hours after supersession.

OTAR/OTAT POLICY

1. Electronically generated key (KG-83) must be tagged/marked in accordance with references (c) and (d) to allow identification of the generated key. A generated key's tag or designator will be assigned by the generating station. The tag will consist of three information fields:

a. Field One. Is a two digit number which represents the consecutive number of electronically generated key produced by the generating station on a particular day. It is assigned 01 at the beginning of each new radio day and advanced by one in sequence for each that follows.

b. Field Two. This field will identify the generating station. NCTS Guam Technical Control will use "WPBFC" as an identifier.

c. Field Three. This field contains the Julian date the key was generated.

2. Per references (c) and (d), elements of NCTS Guam involved in OTAT/OTAR will maintain a station OTAT/OTAR log. This log will be retained for a minimum of 60 days. The OTAT/OTAR log will contain the following items:

- a. Key Source
- b. Key ID/Short Title
- c. Classification
- d. Controlling Authority
- e. Effective Period
- f. Storage Position and Fill Device Serial #
- g. Initials of Two Persons Filling Storage Device
- h. Circuit I.D. Transmitted Over
- i. Date Time of Transmission
- j. Receiving Stations
- k. Initials of Two Persons Conducting OTAT/OTAR
- l. Zeroized Date Time
- m. Initials of Two Persons Who Zeroized Fill Device

GENERATING STATION OTAR/OTAT LOG FOR THE MONTH OF: MMM YYYY

1. KEY SOURCE	2. SHORT TITLE	3. EDITION	4. ALC CODE	5. CLASS	6. EFFECTIVE PERIOD	7. STORAGE POS & FILL DEVICE	8. DATE/TIME OF XMISSION	9. RECEIVINGS TATION(S)	10. ZEROIZED DATE/TIME	11. INITIALS

PAGE ____ OF ____

Derived from: EKMS 1 (Series)
Declassify on: 22 September 2028

“RETAIN FOR 60 DAYS FOLLOWING THE DATE OF LAST ENTRY IAW EKMS 1
(SERIES) ANNEX T”

CONFIDENTIAL

(WHEN FILLED IN)

WATCH-WATCH INVENTORY PROCEDURES

1. Each item will be listed in alphanumeric order and material requiring a page check will be indicated by an asterisk (*) preceding the material short title.

2. Sight all COMSEC material held on watch by short title, edition, and registered number and Accountability Legend (AL) code. For example, * USKAT 12345 Edit C, Reg 678, AL 1 would be accounted for in the following manner:

a. Complete short title

b. Edition

c. Reg Number

d. AL code

e. Ensure the CMS-25 reflects the superseded segment was destroyed and the next consecutive segment appears in the canister window.

f. After verifying all material and equipment are present, the oncoming and off-going watch will sign the watch-to-watch inventory. Supervisors are cautioned these signatures acknowledge all items have been accounted for and are now the responsibility of the section on watch.

3. The inventory will include the following statement:

"I certify that I have personally sighted and inventoried each of the above listed publications/material and have page-checked those indicated by an asterisk. By my signature, I acknowledge responsibility for maintaining security precautions for all above listed publications/material during my watch or until properly relieved."

4. Any discrepancy noted during the inventory shall be reported immediately to the LEC or the EKMS Manager.

5. Watch-to-watch inventories will be retained by the LEC for 30 days.

6. The LEC Custodian will fill out a CMS-25 segmented destruction document or local equivalent prior to issuing any COMSEC keying material to the watch section (refer to Chapter 7, Figures 7-1, 7-2 and 7-3). Each CMS-25 will have the short title, edition, registered number and accountability legend listed exactly as it appears on the material itself for one short title. The CMS-25s will be placed into a folder/binder for the watch section. Use the one that fits the material usage. These forms have been developed to assist the watch section and avoid confusion.

7. Use the key tape Diagraph Codes Fig 2-1 of ref (a), to place the correct number of segments rows on the CMS-25.

Example: Diagraph G = 16 segments (numbered 1, 2, 3, 16)
C = Monthly

In this example one key segment is used each month of the year, and the 13-16th key segments are spares. All key segments will coincide with the rows on the CMS-25 as to prevent confusion.

8. Page checks verify completeness of COMSEC documents, material and publications. Page checks will be accomplished in accordance with reference (a) article 757 and the following:

a. Unsealed COMSEC material must be page checked upon initial receipt, upon transfer, during ALL account inventories, during daily watch-to-watch inventories, and prior to destruction.

b. Sealed keying material, and keying material packaged in canisters, will be verified by comparing the short title and accounting data in the canister window against the same data on the receipt/transfer document (SF-153) and canister segment WILL always be 01, 01/03, or 01/05.

c. Segmented keying material packaged in canisters will NOT be pulled or removed from the canister for page checking.